INDICARE Monitor

ISSN 1614-287X

About Consumer and User Issues of Digital Rights Management Solutions

Volume 2 2005/2006
http://www.indicare.org/monitor

April 2006

Knud Böhle (ed.)

with contributions by INDICARE staff and by Javier Barria, Nicholas Bentley, Mark Bide, Olivier Bomsel, Andrew Braid, Koen Buyens, Karen Coyle, David Crombie, Philippe de Cuetos, Bart De Decker, Arnoud de Kemp, Ellen Euler, Marc Fetscherin, Mia Garlick, Anne-Gaëlle Geffroy, Robert A. Gehring, Brian Green, Rüdiger Grimm, Lars Grøndal, Susanne Guth, Marieke Guy, Christine Hafskjold, Jordan S. Hatcher, Chris Hibbert, Dan Hunter, Renato Iannella, Kiyohiko Ishikawa, Wouter Joosen, Brian Kelly, Till Kreutzer, Dominik Knopf, Dirk Kuhlmann, Tim Kuik, Cornelia Kutterer, Roger Lenoir, Wanqing Li, Zvi Lifshitz, Neil McKenzie, David Mann, Boštjan Marušič, Paola Mazzucchi, Sam Michiels, Lucy Montgomery, Daniel A. Nagy, Jacob Skjødt Nielsen, Laurent Piron, Richard Poynder, Michael Pramateftakis, Jens Redmer, Tobias Regner, Manon Ress, Thomas Rieber-Mohn, Bill Rosenblatt, Timo Ruikka, Rei Safavi-Naini, Martien Schaub, Florian Schreiner, Carlos Serrão, Nicholas Sheppard, Matthias Spielkamp, Tobias Steinke, Péter Benjamin Tóth, Pasi Tyrväinen, Vural Ünlü, Kristof Verslype, Dirk A. Weber, Oliver Welter

INDICARE

The Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe

http://www.indicare.org

eContent

Disclaimer

Copyright

Comments

You are invited to send any comments, critics or ideas you may have on this publication to knud.boehle@itas.fzk.de and to the project co-ordinator at orwat@itas.fzk.de.

Quote

We recommend quoting the present publication as follows:
Böhle, Knud (ed.): INDICARE Monitor, Volume 2 2005/2006. Karlsruhe: 2006;
http://www.indicare.org/monitor

Note

Your are invited to comment on any article of the INDICARE Monitor using the online comment function no matter how long the article is already online. You will find all INDICARE Monitor articles readily available at http://www.indicare.org/monitor.

INDICARE Project

INDICARE – The Informed Dialogue about Consumer Acceptability of Digital Rights Management Solutions – addresses problems pointed out in the eContent work programme 2003-2004: "There has been little attention to the consumer side of managing rights. Questions remain open as to the level of consumer acceptability of rights management solutions" (p. 19). In addition to consumer issues INDICARE addresses the user side, in particular concerns of creators and small and medium-size information providers.

INDICARE maintains an informed dialogue about consumer and user issues of DRM. Informed dialogue means that discussions are stimulated and informed by good quality input such as news information and profound analyses. Options for participation and more information about the project and its deliverables are provided at the project website: http://www.indicare.org

The INDICARE project is conducted by the following partners:

- Forschungszentrum Karlsruhe, Institute for Technology Assessment and Systems Analysis (FZK-ITAS), Project Co-ordination
- Berlecon Research GmbH, Berlin
- Institute for Information Law (IViR), University of Amsterdam
- SEARCH Laboratory, Budapest University of Economics and Technology

Preface

The INDICARE Monitor is the online-journal of project INDICARE being published every last Friday of a month. The present second volume of the INDICARE Monitor contains the 12 issues which have been published during the second year of INDICARE operation (March 2005 – February 2006). It contains more than 100 articles written either by members of the project team or external experts.

To add value to this volume we have included again a *keyword index* and a *name index*. While the keyword index helps to find articles by subject matter, regional focus, and article-type (announcement, case study, conference report, country report, economic analysis, editorial, interview, legal analysis, news analysis, opinion, policy analysis, review, survey, technical analysis), the name index references names of persons mentioned in the articles – not including deliberately names of authors. For this edition all articles have been checked again in order to diminish typos, to apply the layout rules more consistently, and to attribute keywords more carefully. Thanks to *Gabriele Kaufmann*, secretary at ITAS, for the many hours of skilled word processing and layout it took to produce the present publication.

The main purpose of the INDICARE Monitor is to inform on consumer and user issues of DRM solutions in Europe and to stimulate public debate. Debate means two things here: first, the online-journal itself is scheduled as a platform for debate where different opinions and views can be expressed, and secondly articles posted on the INDICARE website can be discussed online straight away.

Some articles reached an audience of almost 1.000 readers at our website within a month. Some articles have already been downloaded more than 7.000 times. As articles can also be obtained by RSS feed and by downloading the whole monthly issue as pdf-file, the effective readership is always larger than the counter of article visits indicates.

A more qualitative measure for the success and the quality of articles is the fact that articles of the INDICARE Monitor are not seldom referenced, commented or syndicated by other web resources, e.g. PaidContent by *Rafat Ali*, QuickLink by *Richard Swetenham*, *Urs Gasser*'s blog at Berkman Center for Internet & Society Berkman Center, *Stefan Bechtold*'s blog at the Center for Internet and Society (CIS) at Stanford Law School, *Charles W. Bailey*'s Scholarly Electronic Publishing Bibliography and Scholarly Electronic Publishing Weblog, or at BillboardPostPlay. Meanwhile the INDICARE Monitor has also been included in electronic journal catalogues and is indexed in Library and Information Science Abstracts (LISA).

The INDICARE Monitor has turned out to be a place of DRM debate,

- where empirical *consumer research* is reviewed and presented,
- where *consumer organisations* and other relevant NGOs have a voice,
- where *young researchers* working on DRM publish original ideas,
- where interesting *interviews with key persons* take place,

– where national and *European research projects on DRM* are covered,
– where the *implementation of the European Copyright Directive* in member states is followed closely,
– where *European and US* debate meet, and
– where you can find information about *DRM events* which are not covered elsewhere (e.g. workshop and conference reports).

The keyword index gives an impression which topics ranked especially high. Conforming to the scope and the focus of INDICARE it is most naturally that the issue of consumer expectations, copyright law, DRMS design, business models, as well as standards and interoperability have been dealt with most often. Special focus themes helped to address in some depth important issues beyond the mainstream discourse such as "DRM and e-payment systems", Trust, DRM, and TC", "DRM and disabled" or "DRM and scientific publishing". In the *Masthead* at the end of this publication (cf. p. 408) you will find more information about the dissemination of the journal, the editorial team, and the editorial policy.

Knud Böhle
(Editor)

Table of Contents

INDICARE Monitor Vol. 2, No 3, 30 Mai 2005

INDICARE Monitor Vol. 2, No 4, 24 June 2005

INDICARE Monitor Vol. 2, No 5, 29 July 2005

INDICARE Monitor Vol. 2, No 6, 26 August 2005

INDICARE Monitor Vol. 2, No 7, 30 September 2005

INDICARE Monitor Vol. 2, No 8, 28 October 2005

INDICARE Monitor Vol. 2, No 9, 25 November 2005

INDICARE Monitor Vol. 2, No 10, 23 December 2005

INDICARE Monitor Vol. 2, No 11, 27 January 2006

INDICARE Monitor Vol. 2, No 12, 24 February 2006

Editorial of INDICARE Monitor Vol. 2, No 1, 25 March 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: With the second year of INDICARE we start the second Volume of the INDICARE Monitor this month. Beginning with the present issue, the Editorial will always fulfil two purposes. It will announce INDICARE project news and it will introduce the respective issue. Apart from payments and DRMs, the current issue continues debate about DRM patents, requirements of the European Copyright Directive (EUCD), and adds a further comment of the first INDICARE State Of the Art Report – this time from the IT-industry side. We also introduce a newly emerging DRM topic, namely the use of DRM systems for computer games, and we present a straight forward economic analysis of DRM by two French researchers involved in the European IST project MediaNet.

Keywords: editorial, INDICARE

INDICARE news

The second INDICARE workshop last month on "E-Payment and DRM for Digital Content", hosted by INDICARE partner SEARCH in Budapest, has been a success in terms of quality of speakers and quality of participants lively debating. It became clear that "paid content" and "protected content" require integration, eventually because consumers want easy-to-use services.

The *workshop report* documenting the event has been released this week and is available online (at http://www.indicare.org/tiki-page.php?pageName=Events). At the same page you will also find the speakers' *presentations*. A *brief summary* of the Workshop, prepared by *Kristóf Kerényi*, is included in this INDICARE Monitor issue.

About this issue

The present issue containing the brief summary of the second INDICARE Workshop already mentioned above, also includes an in depth interview with *Rüdiger Grimm*, one of the speakers at the workshop. He highlights the need for integration of DRM systems and payment system, and the role for payment service providers as intermediaries. He is sceptical about the role of PKI for DRM. In his view PKI and signatures are fine for B2B rights management but not for B2C e-Commerce as long as the infrastructure is not available for other purposes as well. He also warns that "there is a huge privacy bomb out there in DRM services". Both topics are relevant in other articles too, as we will see.

The debate about DRM patents has been taken up already in the last issue with a review of the Berlecon Whitepaper, and an Interview with *Larry Horn* Vice President of MPEG LA by *Thorsten Wichmann*. One of the crucial questions is the patent claim of ContentGuard with respect to rights expression languages and the claim of MPEG LA with respect to essential OMA 1.0 patents. We are delighted that *Susanne Guth* and *Renato Iannella* respond to this challenge and present their open source advocates view. Both are heavily involved in the development of ODRL, which is used among others by the OMA consortium as rights expression language.

The EUCD is addressed in two articles: *Dominik Knopf*, working at the "Institute of Information Law" in Karlsruhe proposes a concept how to implement copyright exceptions in DRM systems. To achieve this, he argues, a paradigm shift: would be required from object-oriented DRMs to user-specific DRMs linking the content to the person, who acquired the rights to use it. By this he contributes to an "emerging scholarship", as *Stefan Bechtold* termed it (cf. INDICARE Monitor, Vol. 1, No 4, 24 September 2004) interested in a value-centred design of DRMs able to preserve important policy and legal values. As Grimm made clear in the interview, as long as the required infrastructure to hook up to is not in place, DRMs proposals like the one by Dominik Knopf – as the author admits – have to be taken as feasibility studies, not as something we will see soon.

Margreet Groenenboom, IViR, reviews a paper by *Urs Gasser* and *Michael Girsberger* on the transposition of the EUCD with respect to the legal protection of technical protection measures. One of the striking points is the spectrum of legitimate interpretations. While, following a *narrow* interpretation, the EUCD only prohibits the circumvention of those TPMs that prevent or restrain uses that are relevant under copyright law, the *broad* interpretation regards any TPM protected which aims at preventing or restricting any act not authorized by the rightholder. This openness of interpretation consequently leads to a lower degree of harmonization among EU member states.

Olivier Bomsel and *Anne-Gaëlle Geffroy,* Ecole des Mines de Paris, provide a clear cut economic analysis of DRM systems. They start from two basic functions of DRM systems: content *protection* and *versioning*. Next they distinguish between two types of networks: "two-way communication networks" like the Internet, where everyone can technically broadcast contents, and "one-way networks" like broadcast networks. The economists hold that the "broadband Internet roll-out is largely subsidized by circumvented contents available through P2P applications". Circumvention would benefit the whole range of IT-industries, which could not be forced to accept DRMs on open networks. The situation seems to be rather different in one-way-networks where content owners "control the availability of contents and the indirect network effects". Here, equipment manufacturers have to accept protection standards demanded by the content industry. The analysis shows that in order to assess the future of DRMs deployment, it is most important to distinguish network types as they frame to a certain extent the chances of stakeholders to push through their respective interests.

Danny Vogeley, Berlecon Research, addresses a rather new topic. Only recently the computer game industry has started to use DRM-based usage control systems. A case in point is the most successful Half-Life 2, which sold more than 1.7 million copies between November 2004 and January 2005. What Vogeley observes is not merely an emerging application field for DRMs. He can show that right from the beginning this technology is used to violate consumer rights. Another interesting observation is, how little consumers have reacted to this practice. In fact it has had no negative effect on sales. This shows how important it is to distinguish application areas and consumer groups considering acceptance and acceptability of DRMs, What might provoke protests and refusal in one area might be acceptable without grumbling in another.

The last article of this issue is again a comment on the SOAR. *Timo Ruikka*, Nokia Corporation, suggests rethinking consumer expectations in a long-term perspective with respect to flexibility and transparency requirements. He also says that the INDICARE paper "has far too great emphasis on privacy aspects, as if DRM was a bigger threat to privacy than (for instance) eBay or electronic banking or credit card statements". This statement sounds quite different from what security expert *Rüdiger Grimm* had termed a "huge privacy bomb out there in DRM services".

Be this as it may, in any case there is still a need for discussion of DRM issues, and INDICARE is the dialogue platform for this purpose. Come and comment the articles on our website and write for the INDICARE Monitor.

Happy Easter!
Knud

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 24/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=91

E-Payment and DRM – Integration needed

A brief summary of the second INDICARE workshop in Budapest, February 3, 2005

By: Kristóf Kerényi, SEARCH laboratory, Budapest, Hungary

Abstract: The second INDICARE workshop on "E-Payment and DRM for Digital Content" took place in Budapest on February 3, 2005. There was good interest in the event, which indicates that e-payment and DRM are topics of equally high interest to both the industry and academia. The workshop provided some revealing insights into the role of e-payment in complex DRM-enabled systems, and also called for better integration in order to create more acceptable systems to consumers.

Keywords: conference report, INDICARE – business models, collective rights management, e-payment, m-payment

Introduction

When we started organising the second INDICARE workshop with e-payment being the intended focus, we thought we would be in a difficult situation, since from the technical point of view e-payment has hardly anything do with DRM. However, we quickly found out that from the consumers' point of view the situation is very different. Consumers do not really bother about technical details, at least they do not wish to. Instead, they are looking for easy-to-discover and easy-to-use services, which provide them with a new experience of consuming digital content in fascinating ways.

Thus recruiting the intended number of a dozen speakers and the optimal number of a half century of attendees for the workshop held in the excitingly modern informatics building of the Budapest University of Technology and Economics was not a difficult task at all.

The workshop was organised around four thematic blocks: "e-payment technology", "service providers on DRM", "content providers in motion" and "business models for consumer satisfaction". Below I attempt to give a very brief coverage on what in my view were the interesting conclusions. Interestingly enough, consumer issues came up in more cases than expected.

E-Payment technology

The first block of presentations was organised around technical questions of e-payment. Traditional e-payment solutions have been in use on the Internet for years, so there is not much current development in that area. However, with the expansion of the mobile market, and with handheld devices making it into our pockets, a transition to m-payment is taking place. This will be even truer as mobile devices open up new opportunities like near-field communication and the use of smart-card-based security.

Risto Sipilä talked about new *touch-based* services based on near-field communication, the so-called *Radio Frequency Identification (RFID)* technology. As opposed to remote payments, near-field communication is based on locality, where new types of point of sale (POS) terminals will accept e-cash or tickets (e.g. cinema tickets) directly from the consumer's mobile phone without having to connect to the mobile network. The speaker underlined two very important aspects when developing new mobile services: on the one hand ease of use was very important, from easy-to-use terminal (phone) user interfaces through easy service discovery to convenient payment methods. On the other hand, besides *user friendliness* he urged for *open technologies* and *open standards*.

Péter Papolczy talked about SEMOPS (Secure Mobile Payment Service), a research project funded under the 6th Framework Programme for Information Society Technologies of the European Union. SEMOPS is a new concept for a *real-time payment service*, which can be implemented across a variety of mobile devices or other handsets,

over different data carriers and for a large spectrum of payment amounts. SEMOPS is differentiated from other e-payment services by its consumer-centric design. It provides consumers as Papolczy claimed with unprecedented *flexibility*, while also ensuring *privacy*. SEMOPS combines consumer anonymity with refundability. This is a quite new approach to e-payment, since so far in every widespread solution the consumer has been traceable.

Service providers on DRM

In the second block of presentations two speakers brought forward their views on the provider side of e-payment and DRM. The first of them, *Pál Miletics*, who came from a major mobile service provider, presented facts and figures about the mobile telephony market and the mobile market in general. In his view, customers demand services for information access, content download, ticket purchase, parking payment, or ordering. He underlined that there was a big difference between traditional e-commerce and m-commerce, the latter providing anytime-anywhere type services limited only by the handsets' capabilities. He also said that consumers usually do not understand the benefit of new technologies, so accurate surveying of market needs would be very important in order to succeed with DRM services.

In the second presentation by *Tamás Foltányi*, the attendees heard about a selection of case studies from the technology provider's point of view. The speaker pointed out that the mobile business environment is *significantly different* in the United States, in the EU and in Eastern Europe, so care must be taken when one wants to talk about *business opportunities* in general. He said that consumer interest in e-payment services is present, as is the technical background, so using e-payment is not a problem. However, when analysing opportunities, one must look at the whole "value chain".

Content providers in motion

The first presentation in the third block was about general DRM issues, more specifically the aim of DRM. *Tibor Sas* first looked at DRM from the *infrastructure* point of view and regarded DRM as infrastructure for the management of rights. He concluded that also for the DRM infrastructure a critical mass of consumers would be necessary to pay off. Second, he emphasised the *importance of object identification*, and proposed the widely used Digital Object Identifier (DOI) as a means of solving several DRM-related problems, especially the collection and distribution of fees as a main purpose of the DRM infrastructure. He also brought up several use cases with inherent problems, e.g. component reuse, print-on-demand of small-volume publishing and mixed-financed learning materials. He came to the conclusion that object identification and DRM could solve these, especially by identifying, tracking and billing uses of the many small-scale components by many parties. Finally, the speaker pointed out that in his view the chief problem was the lack of e-content materials in the appropriate quantity and quality. He concluded that a working DRM infrastructure and intensive content protection would encourage providers to supply more valuable content.

Péter Benjamin Tóth, a lawyer at a collecting society of authors and publishers gave a presentation on the role of collecting societies in a world of DRMs. The main issue of the presentation was whether with the spread of DRM systems collecting societies will die out, or whether collective rights management still has some future. He asked if DRM and levies can coexist, and if it makes sense to use DRMs to make royalty distribution more accurate. The answer, he said, might be given by the International Confederation of Societies of Composers and Authors. CISAC's aim is to develop documentation and distribution standards for the sake of better accounting between collecting societies. CISAC works together with ISO, and they have developed accepted standards for the identification of works and rights holders, which actually forms also the basis of every DRM system.

Business models for consumer satisfaction

The last block of the day started with an analysis of DRM business models. The speaker *Vural Ünlü* categorised content protection strategies into three groups: *technical* protection, *contractual and statutory* protec-

tion and the alignment of business models forming *structural protection* for content. The speaker then analysed the optimal level of technical content protection. His conclusion was that *valuation* and *content degradation* are major determinants of this optimal level, which also rises with the *network effect*. Two further findings were that the profit of content providers is reduced when protective measures cause *utility decline* for consumers, and that the alignment of business models may lead to additional revenues.

Rüdiger Grimm talked about a conflicting situation between content providers and their potential customers when it comes to digital products available on the network. He examined several alternative business models, among them systems based on Light Weight DRM, the PotatoSystem, and Music2Share. The particular feature of the PotatoSystem is to allow reselling by customers and thus providing incentives not only to legally buy digital products but also to contribute to the distribution. The speaker talked about digital payment methods having to be integrated into the purchase procedure. He pointed out that payment is not integrated in most of the existing DRM systems, and that this is a mistake. LWDRM and the PotatoSystem, in contrast, have payment integrated in the purchase procedure, he said. His conclusion was that a great number of consumers are ready to pay for fair use, and providers are ready to deliver content for payment, so a *mutually acceptable level* of payment is the key. Therefore, he said, *payment has to be integrated with DRM* and free usage has to be enabled after payment. Finally, he called for a harmonised solution, technically standardised and widely accepted on the market.

Main conclusions

Perhaps the main conclusion of the workshop was that e-payment solutions must be integrated into the content purchase process. And of course if DRM is also used, e-payment has to be integrated with DRM, too. Consumers do not want to bother about technical and contractual details, they just want to see the offer as one product and then they can decide which one to choose. Of course with today's technical advancements in mobile computing and wireless connectivity traditional e-payment is shifting over to m-payment. Integration is even more important here, since consumers have already got used to the "one finger, two buttons, three clicks" rule. Any other, more complicated purchase method will be less successful.

Another key result of the workshop was that more attention should be given to consumer needs and consumer wishes. However, it is difficult to establish what they want, since they, themselves, do not know exactly what the possibilities are. Also, fair use should be considered in depth when creating new models for consumers: alternative compensation systems, like the described PotatoSystem, could have a bright future. Finding the perfect offer for consumers is, and will stay a key challenge for markets depending on DRM-protected contents.

Bottom line

If you have more interest in the Budapest workshop, please look at the *workshop-site* where you can download the slides of the speakers' presentations. You might also want to read the more extensive *workshop report* (Jeges and Kerényi 2005) – it will bring you all of the interesting points of the presentations and of the panel discussions in detail.

Sources

- Jeges, Ernő and Kerényi, Kristóf (ed.) (2005): E-Payment and DRM for Digital Content – Report on the 2nd INDICARE Workshop, Budapest, 3 February 2005; http://www.indicare.org/tiki-download_file.php?fileId=98
- Workshop-site: http://www.indicare.org/events/

About the author: *Kristóf Kerényi* is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His interests include mobile and wireless IT security, as well as technological aspects of DRM. He received a MSc in computer science from BUTE. Contact: kerenyi@mit.bme.hu

Status: first posted 22/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=89

Where do DRM- and e-payment systems meet?

By: Rüdiger Grimm, Technical University Ilmenau, Germany

INDICARE-Interview by Knud Böhle, ITAS, Karlsruhe, Germany with Rüdiger Grimm, Technical University Ilmenau, Germany.

The interview approaches the relation of DRM systems (DRMs) and payment systems from different angles, addressing aspects of technical integration, the need for micropayment-systems, strategic partnerships, the role of payment intermediaries in content markets, and takes a look at the near future.

Keywords: interview – business models, e-payment, micropayment, privacy

About Rüdiger Grimm: *Since September 2000 he has been professor for multimedia applications at the Technical University of Ilmenau, Germany. He also heads a research group at Fraunhofer (IDMT – Fraunhofer Institute for Media Technology). Research interests include trustworthy and secure e-commerce applications, payment systems, business protocols, privacy and digital rights. Among the solutions he has contributed to are numbered the First Virtual payment system, and more recently the PotatoSystem and Light Weight DRM. Contact: ruediger.grimm@tu-ilmenau.de*

INDICARE: A payment function is often regarded an important component of a DRM system. Nevertheless it seems as if there is not much communication and overlap between those dealing with e-payments and those dealing with DRMs. You are expert in both fields – would you agree that both communities are strikingly separated?

R. Grimm: There are two communities, partly but not completely separated. Indeed, there are a lot of "kernel" DRM systems which are not closely linked to a business model, such as Windows Media Rights Management, Helix, Atrac3 or Fairplay. Also, payment systems like PayPal or Moneybookers are not directly involved in digital goods download through a DRM system. In addition there are also business models for protected content, like iTunes and Sony Connect, not associated with a strategic e-payment system. In this respect: yes, there are two different communities which are only partly interlinked.

But there are other examples of strong interrelation between these communities: The business model of the e-payment system Firstgate's Click&Buy aims at digital goods. During the payment process the purchased digital goods are tunnelled through the server farm of the payment system. This is a DRM business system. The same is true for Paybest. Paybest is closely linked with the PotatoSystem. There is no Potato download without stepping through the Paybest process. The provider of Paybest and the PotatoSystem is the same firm. And iTunes in the US (not in Europe) offer payment by PayPal, as a first step to electronic payment integration.

INDICARE: This means that on one side we see companies who follow an integrated approach with a business model for virtual goods in mind, and on the other side we observe an approach where different components are integrated *ex post* at the level of the eCommerce system. Why ask for co-operation and a common view if in practice there is no need for joint action and joint systems development?

R. Grimm: I see two reasons why the two strands are not always integrated. Number one is the reason you mention: DRM is in the first place a technical mechanism. Only within a digital goods business system, is payment required. Nonetheless, iTunes is indeed a business system, and – in Europe – it is not interlinked with an electronic payment system. Number two is that both parties, payment systems and DRM business systems, have their own customers. It is not easy for one of the two parties to serve the customers of the other. Both want to serve their own customers. However, this situation is uncomfortable for all users. It limits mar-

ket growth for both sides. Therefore, it is a matter of time until successful download or file sharing systems conclude strategic partnerships with specific payment partners. Just like eBay goes with PayPal, payment systems will concur to become strategic partners of successful download or (legal) filesharing systems.

INDICARE: Neither PayPal (with eBay) nor credit card payments (with iTunes) are micropayment systems. Do eContent markets need micropayment systems at all?

R. Grimm: Yes, they do. Payment must be (a) strongly interwoven with the purchase process, (b) immediate and able to conclude the purchase, (c) cheap enough for low-price eContent. But there are interesting other models beyond micropayment, such as packeting several purchases to one payment, or subscription, which make credit card payment cheaper.

INDICARE: How big is the demand for integrated DRM & E-payment systems and what are the most successful systems today?

R. Grimm: Successful digital goods purchase systems will provoke Internet micropayment systems. As mentioned above, FirstGate Click&Buy is a functioning integration of micropayment and download of digital goods. Paybest and PotatoSystem is another example. PayPal and Moneybookers are prominent candidates for strategic partnerships with download shops, because they do have a broad customer base. iTunes in the US have already started with PayPal.

INDICARE: Listening to all the names the question of interoperability as a condition for a unified consumer experience automatically pops up. Won't we see again lots of incompatible islands? How will the interoperability problem be solved if not by a winner takes it all logics?

R. Grimm: Exactly so. There are so many different DRM solutions on the market, and they are all incompatible. Electronic payment is not much better. Accounts from one system cannot be used to pay with another system. So, customers get used to having as many logins, accounts, contracts and rules as they use download services and payment systems. To top this problem: They all play with the personal data of their customers. There is a huge privacy bomb out there in DRM services…

INDICARE: What exactly do you mean by "privacy bomb"?

R. Grimm: Web surfers purchase more and more virtual goods. Traces of personal data are created by communication with servers, and also in encoded form within the products. Mostly people are not aware of this networked information about their behaviour. Nor is it utilized so far. However, the information is out there, and it is increasing every day. Users should insist on being informed on the usage of their data. And providers of services should know that trust is the most important basis of business, therefore it is worthwhile to provide transparency on their actions.

INDICARE: Back to payments, do you think it is possible to draw lessons from the early internet payment systems like First Virtual, eCash and CyberCash for the design of DRM systems?

R. Grimm: All three systems worked as both, payment, and digital goods purchase. In modern language: they managed digital rights. But they were not DRM systems in the narrow sense: there was no copy protection or usage control involved. But nevertheless there are (at least) three lessons to learn: (1) payment and digital goods purchase must be simple and cheap: no public key registration or so! (2) There must be many goods of accepted value available on the Internet; (3) there must be no privacy threats.

INDICARE: You mentioned public keys. PKI is debated today in the context of DRM too, when it comes to the granting of exemptions from the owner's exclusive rights. At the last DRM conference in Berlin (see Orwat 2005) Thomas Dreier for example envisaged a solution to this problem through DRM systems based on PKI. What is your opinion on a PKI based DRM approach to achieve fair use?

R. Grimm: PKI are heavy weight for handling. PKI and signatures are fine for B2B rights management. Customers will avoid the

extra load of care they have to take for their keys. PKI will be a solid basis for B2C e-Commerce if it is available and used for other purposes as well. But this is not yet in sight.

INDICARE: Well, in other words this means PKI and TTPs are not appropriate means to enable users to enjoy their traditional rights, like making private copies, granted by copyright? Do you have a better solution in mind how to reconcile DRMs and the legal provisions?

R. Grimm: Trusted Third Parties as service providers to enforce additional rights or other services (like fair exchange of high-value) might indeed be an appropriate business model. But PKI for key management just in order to sign contracts is an overload on digital goods, especially in the low value range.

INDICARE: From PKI to payment systems infrastructure is just a tiny step. Payment systems and also micropayment systems at the end of the day need a channel to communicate with the banking world and the monetary system. This missing link has been a problem for micropayment systems, is it an issue for DRM systems? Asked differently, what is the role for payment intermediaries in the field of paid protected content?

R. Grimm: The intermediaries must be the payment systems themselves. It is the purpose of an e-payment system to map the heavy-weight banking system into light-weight Internet communication. They organise intermediate accounting to bundle payment processes for clearance in the "real money world" of banks. When they do this, they offer additional services such as reporting, control of download, re-load of lost goods, concluding a purchase.

INDICARE: Talking about technical infrastructures, there are (apart from convergence) still different types of networks: the open Internet, mobile phone networks and digital TV. Can we expect to see in the future most paid content via digital TV und UMTS mobile networks?

R. Grimm: The mobile world is special. Mobile phones are easier to protect against tampering. Individuals accept to pay for access to mobile networks. Mobile devices carry individual IDs for tracking and accounting. Bringing these points together, mobile networks are predestined for DRM-protected download and payment. Paid download of ring tones works extremely well. Therefore, the mobile industry has great hope, that it will be accepted as a digital goods purchase world. However, this will only succeed if the systems are compatible. OMA - the Open Mobile Alliance - is the relevant standardization initiative. Without success of OMA there will be no mobile DRM business.

The TV world is completely different. I don't see a strong overlap between the passive-consumption world of TV with the active consumption world of the B2C e-commerce – at least in the near future. This might change, but not very fast.

INDICARE: By and by p2p-Networks are being recognized by eContent industries as an opportunity (see Rosenblatt 2005). How will adequate payment systems look like for P2P networks? Can we envisage p2p networks as exponential "recommender-systems" with a payment function?

R. Grimm: A view into the near future, as I see it: Payment systems for digital goods within p2p-networks play the role of intermediaries between p2p value exchange and the real banking clearance. The payment system collects different payment activities and does the intermediate accounting before clearance. All services, such as provisions and special offers are managed by the payment service. Payment customers have access to a huge set of digital goods offerings.

INDICARE: By the way, can you imagine upgrading your PotatoSystem to p2p networks?

R. Grimm: Yes, PotatoSystem is prepared for an upgrade to p2p communication. This requires a close inter-play with an e-payment service, just as Paybest today. Already today Paybest is a broker for many other e-payment services such as Paysafecard, Micromoney, Moneybookers, and Click&Buy.

INDICARE: Isn't it amazing that we have talked all the time about DRMs without even

mentioning copy protection? Looks like entering the DRM arena through the payment door you automatically think of DRMs in terms of business models…

R. Grimm: Virtual goods are made for purchase and usage, not for being protected against usage. It is indeed amazing, that content providers emphasize copy protection and forget so much about new opportunities to make money. Payment brings it all together: content providers want money and consumers want products. Instead of raising border walls of usage protection between them, content providers should open payment doors to their customers and make their goods accessible – and consumable.

INDICARE: Thank you very much for this interview.

Sources

- Information about the PotatoSystem mentioned several times is available at http://www.potatosystem.com/info/eng/index.html
- Rosenblatt, Bill (2004): Learning from P2P: Evolution of business models for online content. INDICARE Monitor, Vol.1, No 6/7, 17 December 2004; http://www.indicare.org/tiki-read_article.php?articleId=61
- Orwat, Carsten (2005): Report on the 3rd DRM Conference, Berlin, 13th and 14th January 2005 INDICARE Monitor, Vol.1, No 9, 25 February 2005; http://www.indicare.org/tiki-read_article.php?articleId=75

Status: first posted 15/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=86

Critical review of MPEG LA software patent claims

The usage of open source rights expression languages must be royalty free

By: Dr. Susanne Guth, Vienna, Austria and Dr. Renato Iannella, Brisbane, Australia

Abstract: This article shows a current software patent case where the MPEG Licensing Administration (MPEG-LA) is claiming license fees for the implementation of the (open) rights expression language ODRL. ODRL has been developed by the international ODRL Initiative, a non-profit initiative mainly run by researchers. The article critically discusses the patents for rights expression languages and introduces early publications, showing that the concept of "rights expression languages or a rights grammar" is not new. Furthermore, it examines the patent claims with regard to the Open Mobile Alliance (OMA) DRM. The article is concluded with a discussion on the potential future impact of software patents in the field of DRM for open source software, research and consumers.

Keywords: technical analysis – competition, open source, patents, rights expression language

Introduction

In January 2005 the MPEG Licensing Administration (MPEG-LA) announced the terms of a joint patent portfolio license to be offered to implementers of the Open Mobile Alliance (OMA) DRM 1.0 specification. A royalty payment of USD 1 is due for every device that is issued using the OMA DRM specification and a further 1% of any transaction in which an end user pays for delivery of a digital asset (cf. MPEG-LA, 2005). From this patent portfolio, we are reviewing the patents that are related to rights expression languages (RELs), e.g. the European Patent EP 0 715 244 B8 respectively the US Patent 5,715,403 "*System for controlling the distribution and use of digital works ... utilizing a usage rights grammar"* granted to the Xerox Corporation. Today the patent is controlled by the US Company ContentGuard which is owned by Microsoft, TimeWarner, and

Thomson. These patents are obviously important in the MPEG-LA patent claim case, as the CEO of ContentGuard recently stated:

> "The OMA didn't choose to use our technology for implementing its Digital Rights Language for OMA 1.0, and instead chose to use a system developed by IPR systems in Australia. We told them that this wouldn't mean that they could escape our patent portfolio and we've been telling them that all along" (cf. Faultine, 2005b).

The "system developed by IPR systems in Australia" identifies the Open Digital Rights Language (ODRL). For many years, the authors of this article developed with many collaborators the Open Digital Rights Language (ODRL). Version 1.1 of ODRL (part of the OMA 1.0 and OMA 2.0 specifications) has been implemented; license tools for ODRL have been created, and devices embedded with ODRL. With the experiences of this and other work, the ODRL Initiative members have improved and extended the ODRL data model and are creating profiles to integrate ODRL and adjacent metadata standards. The ODRL Initiative is about to publish these new research findings in ODRL Version 2.0. The new version meets all gathered requirements from the last years of experiences, and it will make the usage, implementation and processing of rights expression languages more efficient and less ambiguous and takes a step towards more interoperability between the different existing RELs. This ODRL research has mostly been supported by European and Australian research funding and was intended to be made freely available (under open licenses) for other researchers worldwide.

The MPEG LA patent claims state that every service provider or device seller that implements the open source rights expression language ODRL as per the OMA DRM specifications shall be obliged to pay a levy to the MPEG-LA consortium members. As ContentGuard claims to hold patents on *any* REL, not just only their own solution XrML (see also Böhle 2005 and Berlecon Research 2005), it is unclear on the extent of the patent claims to any version of ODRL (now or in the future) and other machine-based languages, such as the open and free Creative Commons licenses. At present, the MPEG LA patent claims seem targeted at OMA DRM implementations only and do not seem to apply to other (non-standard) DRM implementations on mobile devices and services.

The business model of open source is to freely distribute software and technical specifications and earn money with consulting and other services. If the implementation of ODRL or the simple usage of ODRL tools leads to potential royalty payments, the attractiveness of ODRL will shrink and the further work of the ODRL Initiative is seriously jeopardised. RELs like ODRL are gaining importance in University and European research projects for the creation of platforms to distribute learning material (script, slides, and examples) (cf. EducaNext 2005).

Rights expression languages are only a small building block of the Digital Rights Management Technology but all other components of DRM systems are most likely affected by software patents in the same way. This article will focus on the specific case of above named patents on rights grammars to illustrate problems and confusions arising from software patents.

What is a rights grammar?

As ContentGuard claims to hold a patent on *any* rights grammar, at this point one has to pose the question: What exactly is a rights grammar? ContentGuard always uses the term "rights grammar" synonymously with "rights expression language". Linguists would probably not agree here in the first place, however, a rights expression language is a *language to express usage or access rights for parties over assets*. A simple rights expression in ODRL granting the user sguth the right display for the asset proceedings2005 looks as follows:

```
<rights>
 <agreement>
  <party>
     <context>
          <uid>sguth</uid>
     </context>
  </party>
  <permission>
```

```
      <display/>
  </permission>
  <asset>
    <context>
          <uid>proceedings2005</uid>
        </context>
  </asset>
 </agreement>
</rights>
```

But also consider these two examples:

- If the system administrator of a Linux Server sets the "group" rights of file Z to "read, write, execute", he is using some kind of rights grammar.
- If, in a running computer system, four software objects of an access control mechanism, e.g. the party object drmUser, the asset object musicFile, the permission object play, and the constraint object untilTomorrow are related to each other and therewith constitute a rights expression, the system uses some kind of object-oriented rights expression language, too.

Do the REL patents now apply to access control software in general? Numerous copyrighted works that describe access control mechanisms and their implementation, such as discretionary access control (access control lists, capabilities), role based access control, etc. were published long before the filing of the ContentGuard patents. Countless research papers also include formal models with respect to computer system security (cf. Landwehr 1981and Burrows et al. 1991).

Most rights expression languages existing today are technically defined in XML schemas. Not using an XML-based rights expression language simply means that you grant or deny access rights with former programming means, i.e. access control information that is captured in software objects or variables, as shown in the two examples above. The following section will try to clarify the coverage of so-called software patents, particularly with respect to the above mentioned patents on rights grammars.

Investigation of ContentGuard patents with regard to (European) patentable inventions

> "European patents are granted for any inventions which are *susceptible of industrial application*, which are *new* and which involve an *inventive step"* (cf. European Patent Convention, 1973).

Please note that the proposed software patent directive (cf. European Commission, 2002) in the EU has not yet passed the EU parliament. The European patent of ContentGuard has been filed under the Convention on the Grant of European Patents of 1973.

In the current European jurisdiction "programs for computers" are not patentable unless they are new and provide a *technical contribution* or *further technical effect* to the prior art. Additionally, to be patentable, an invention must have *technical character* and must be *non-obvious*.

- The invention must have overall ***technical character***. This means that the invention must use technical features and solve a technical problem. For example, software running on a computer has technical character.
- The invention must be a new ***technical contribution*** or ***further technical effect***, i.e. a solution of a technical problem, e.g. an improvement of computing efficiency.
- The invention must be ***non-obvious***, i.e. the invention must be beyond state-of-the-art and non-trivial for an expert in the field.
- The invention must be ***new***, i.e. the applicant of the patent must be the originator of the invention (i.e. not prior art).

In the following paragraphs, we would like to address the named requirements with respect to the above mentioned patents on rights expression languages.

Technical character

What would a software patent in the EU have to look like that applies to *any* rights language if the invention must have overall *technical character*? Such an invention would have to include the underlying data model, the technical specification and implementation of all today's and tomorrow's rights expression languages. The current rights expression languages already serve different domains (music industry, publishing industry, education), have different focuses (licenses, tickets, contracts), thus have

varying data models resulting in diverse technical specifications, XML schemas, and implementations. The above named patents need to be investigated with regard to this requirement.

Technical contribution and non-obvious invention

Some facts: In 1969 the first mark-up language (GML) was developed by Goldfarb, Mosher, and Lorie followed by the Standard Generalized Markup Language (SGML), becoming ISO standard in 1986 (cf. ISO 1986). The successor of SGML is XML (eXtensible Markup Language) respectively XML schema. Today, mark-up languages are widely used and state of the art. The important inventions and copyrighted work in the field of access control were published in the 1960s and 1970s.

Rights expressions have existed since humankind can talk. The example: "I lend this book to you until tomorrow" is a human readable example of a rights expression language. Is a machine readable example of this rights expression language a technical contribution to the state-of-the-art if neither the means of writing (XML) nor the content (access control expression) is new? Since mark-up languages are state-of-the-art, experts use them to describe all kinds of things: books, individuals, and also rights. As mentioned above, common rights expression languages, including MPEG REL, XrML and ODRL, use XML Schema for their serialization. XML Schema can be regarded as state-of-the-art technology. General, freely available XML parsers can be used to interpret and process MPEG REL, XrML and ODRL rights expressions.

New (prior art)

For a patent to be accepted, it must pass a number of key requirements as outlined above. These include that no "prior art" in this invention currently exists. The process to determine these requirements are "self determined". That is, the patent applicant argues in the proposal that the invention meets these requirements. The patent administrator must make a judgement call based only on this information as they are not experts in the area of the invention.

In the case of the ContentGuard patent ('403) – filed on November 1994 - a number of prior art inventions where overlooked. In particular, the well-known work of Ted Nelson's Xanadu project from the 1980s (cf. Samuelson & Glushko, 1991) clearly a decade before the '403 patent submission. Nelson's work is "novel in proposing to use a contract-based scheme for commercial distribution of written texts" and was also novel in "charging for each and every *use* of their documents" rather then each *copy*. The Xanadu project used an "intuitive *rights-to-do* framework", that is, a system that enabled the user rights to be described for content that limited its use. Strangely, the '403 patent references only a 1994 work of Ted Nelson but does not discuss it.

The European ESPRIT Project "Copyright in Transmitted Electronic Documents" (cf. The CITED Project) from 1990-1993 developed a model that provided control, policing and remuneration, in respect of the use of copyrighted material stored and transmitted in digital form. The project demonstrated and implemented software with mechanisms such as "The Use Right Collector (URC) that collects and manages the use right data base and links the data with their associated rights".

Henry H. Perritt (1993) wrote about the concept of "permissions headers" in which rights information would be attached to every digital work distributed across networks. He indicated that "this representation problem may benefit from the use of some deontic logic, possibly in the form of a grammar developed for intellectual property permissions."

Summary

From this understanding, we conclude that a patent on *any* rights expression language is not possible under current European jurisdiction and would be highly doubtful worldwide. Such a patent would only be relevant to the specific implementation that it describes. The technical implementations of DRM systems today differ widely from the ideas over a decade ago. The original '403 patent authors at Xerox had a "print industry" view of the world and probably would not have even contemplated that a REL

would one day be in a small mobile device managing music delivery. Therefore, open source rights expression languages must be untroubled by the software patent levy.

Examining the ContentGuard patent claims with regard to OMA DRM

MPEG-LA claims that their patent portfolio applies to the OMA DRM standards and a license must be obtained. MPEG-LA has not released the full list of the patents in question and how/where they apply to an OMA DRM implementation. One needs to take it "on faith" that all the patents do apply.

If we look at the details of the '403 REL patent as an example, some interesting facts are revealed:

Patent '403 claims that "Digital works and their attached usage rights are stored in repositories" and "The enforcement elements of the present invention are embodied in repositories" and defines repository functions to include "… store digital works, control access to digital works, bill for access to digital works, loan digital works or automatically handle the commercial reuse of digital works, and maintain the security and integrity of the system". The model is clearly one of advanced repositories undertaking the major functions of the DRM transactions. In the mobile world, it is unlikely that a DRM client on a mobile phone would fall into the category of a "repository" as defined by patent '403. Additionally, the "enforcement elements" of OMA DRM are provided by encrypting the content and storing the keys in separate protected licenses. The OMA DRM model does not use a "repository" to request and allow access to content as this is handled by a client application on the handset.

Patent '403 claims that "A key feature of the present invention is that usage rights are permanently *attached* to the digital work" and that "It is fundamental to the present invention that the usage rights are treated as part of the digital work." This is quite the opposite in OMA DRM implementations. The content and license (usage rights) are separate data files and are never "permanently attached" to the content. Additionally, with superdistribution in OMA DRM, the content is sometimes not associated with any "usage rights" until after purchase.

Patent '403 claims that "The usage rights language is based on the grammar described below. A grammar is a convenient means for defining valid sequence of symbols for a language." The grammar of the OMA DRM licenses is based on XML, and more formally on XML Schema, which has its basis on the DTD (Document Type Definition) from SGML developed in the 1980s, and does not resemble the grammar in the '403 patent.

These are just a few examples of aspects of the '403 patent that need careful analysis for their applicability to current implementations of DRM systems.

Discussion

Is the MPEG LA patent portfolio removing uncertainty?

The MPEG LA is pooling (DRM) patent owners and offers implementers of patent affected (DRM-)technology a patent portfolio for a certain price (such as USD 1 per device and 1% of the digital asset's cost). The Vice President of MPEG LA states that "a patent portfolio assists in removing the uncertainty surrounding the 'patent overhang' " (cf. Horn, 2005), i.e. it is a convenient and efficient way to access the (DRM) technology. On the other hand the patent pooling makes the patent claim non-transparent. In the OMA DRM case it is not clear which patents apply to which parts of the OMA DRM specifications. What consequences would it have if the '403 patent claims with respect to rights grammars turn out to be unjustified? To what extent would that reduce the patent levy? What about all the other patents in the portfolio? Who provides an independent analysis of them? From this point of view the pooling of patents probably causes rather than removes uncertainty.

In the latest news, the Mobile Entertainment Forum (MEF) announced that is has issued a statement regarding the licensing program proposed by MPEG LA for Mobile Digital Rights Management (Mobile DRM) saying that: "The terms being considered by MPEG LA … could have a devastating effect on any

business involved in mobile and wireless entertainment" and "that MPEG LA's proposed royalty rates are onerous, impractical and unclear" (cf. w/o, 2005).

What are the possible consequences for the customer?

- It was the aim of the Open Mobile Alliance to develop an *open* standard, to minimise any impact of patents, and to eliminate royalty payments (cf. Buhse 2004). Hence, all players in the mobile industry had a high motivation to support and implement this standard. Now, device sellers and service providers have been faced with a new potential royalty payment to MPEG-LA - significant additional costs that have not been calculated in their business models. This may also lead some vendors to continue to implement their proprietary DRM systems as there is little benefit in moving to the "open" standard. In this case the customers would have to bear the consequences of non-interoperable mobile phones.
- If the claims of MPEG LA can be imposed (and software patents continue to be granted), the additional costs of the above mentioned patent levy will be transferred to the customer. The latest news about the adoption of software patents in Europe (cf. The Copenhagen Post 2005) shows that software licensing will be an important future business of large software companies.

What are the consequences for the ODRL Initiative and Open Source Developers in general?

If the claims of MPEG LA are validated, the work of the ODRL Initiative and other RELs such as the Creative Commons Licenses will be critically endangered. No open source developer would have a motivation to work on new concepts and implementations for RELs if the royalties for their application are paid to a different organisation. This would mean that open source developers, researchers and universities would have to now constantly monitor and review software patents in future. They will have to apply for patents themselves in order to make research freely available for the public and other researchers. This is costly (maybe not realizable with the restricted budgets at universities) and time consuming (i.e. disables progress). Additionally, the many software patents are an unpleasant surprise for researchers (and others) that started their work in a software patent free environment and are then faced with the fact, that maybe a large part of their work is not sufficiently protected by copyright. This has happened in Standards groups previously and has earned the name "submarine patents' – that could surface at any time in the future.

Bottom line

From the concrete case above we can summarize that more transparency is needed with respect to the legal basis of software patents and its application to DRM technologies. The MPEG-LA patents have the clear potential to disturb research and development in the field of RELs and other DRM technologies. Furthermore, the MPEG-LA patent claims have a negative effect on the growth of European mobile (entertainment) industry. This article is also an appeal to politicians and patent offices to rethink the proposed software patent directive in the EU.

Sources

- Berlecon Research (2005): DRM, DRM Patents and Mobile DRM, Berlecon Whitepaper, http://www.berlecon.de/output/en/studien.php?we_objectID=207
- Böhle, Knud (2005): Obscurity in Patent Matters, INDICARE Monitor, Vol. 1, No 9, http://www.indicare.org/tiki-read_article.php?articleId=82
- Buhse, Willms (2004): Open DRM standards for interoperable mobile services, INIDICARE Monitor, Vol. 1,No 3, http://www.indicare.org/tiki-read_article.php?articleId=37
- Burrows, Lampson, Plotkin (1991). A Calculus for Access Control in Distributed Systems. Advances in Cryptology -- CRYPTO '91, Springer-Verlag (August 1991), pp 1-23
- Coverpages (2005), Patents and Open Standards; http://xml.coverpages.org/patents.html.
- Creative Commons: http://www.creativecommons.org

- European Patent Convention (1973), Convention on the Grant of European Patents, Art.52, Patentable inventions; http://www.european-patent-office.org/legal/epc/e/ma1.html#CVN
- Faultline (2005a) : ContentGuard talks DRM futures, The Register; http://www.theregister.co.uk/2005/01/19/contentguard_drm/
- Faultline (2005b) : Mobile DRM Levy Hits Operators Where It Hurts, The Register; http://www.theregister.co.uk/2005/01/19/mobile_drm_levy/
- Horn, Lawrence (2005): MPEG-LA's portfolio license – A jumpstart for DRM-based markets?, INDICARE Monitor, Vol. 1, No 9, http://www.indicare.org/tiki-read_article.php?articleId=81
- ISO (1986) Standard. No. 8879. Information Processing -- Text and Office Systems - Standard Generalized Markup Language (SGML), http://www.iso.ch/cate/d16387.html
- Landwehr (1981): Formal Models for Computer Security, ACM Computing Surveys, Vol. 13, No.9
- MPEG-LA (2005): News Release, MPEG LA Announces OMA DRM Patent License Terms; http://www.mpegla.com/news/n_05-01-06_drm.pdf
- Perritt, Henry H. (1993): Knowbots, Permissions Headers and Contract Law. Proceedings of the Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment Conference. April 2-3, 1993; http://www.ifla.org/documents/infopol/copyright/perh2.txt
- Samuelson, Pamela; Glushko, Robert J (1991): Intellectual Property Rights for Digital Library and Hypertext Publishing Systems: An Analysis of Xanadu. ACM Hypertext 1991 Proceedings, December 1991, pp. 39-50
- The CITED Project website is available at: http://www.newcastle.research.ec.org/esp-syn/text/5469.html
- The Copenhagen Post (2005): Bill Gates threatens to close Navision in Denmark, http://www.cphpost.dk/get/85881.html
- The EducaNext Platform (2005) website is available at: http://www.educanext.org
- The European Commission (2002): Directive of the European Parliament and of the Council on the patentability of computer-implemented inventions http://www.europa.eu.int/comm/internal_market/en/indprop/comp/index.htm
- The Open Digital Rights Language (ODRL) Initiative, website is available at: http://www.odrl.net
- The Open Mobile Alliance (OMA) website is available at: http://www.openmobilealliance.org
- The Project Xanadu website is available at: http://www.xanadu.com/
- w/o (2005): MEF Issues Industry-Wide Position on MPEG LA's Proposals for DRM Licensing, Business Wire, News of 21. March, 2005; http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20050321005243&newsLang=en

About the authors: *Susanne Guth* received her master's degree in information systems from the University of Essen (Germany) in 2000. She specialized in software techniques and production/operations management. Since August 2000, she has been an assistant professor in the department of information systems at the University of Economics and Business Administration in Vienna, Austria. For the last four and a half years, her research focus has been on contract and rights management for digital goods. She wrote her doctoral thesis in this field. Susanne Guth is a private, active member of the ODRL Initiative, leading the development of ODRL Version 2.0.

Renato Iannella is a researcher at National ICT Australia (NICTA). he has extensive experience in the development and standardization of Internet, Web, and mobile technologies and was a former member of the World Wide Web Consortium (W3C) Advisory Board. He is also visiting associate professor at the University of Hong Kong and was previously the chief scientist at IPR Systems and principal research scientist at the Distributed Systems Technology Centre (DSTC).

Status: first posted 22/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=90

Economic analysis of DRMs roll-out over the Internet

By: Olivier Bomsel and Anne-Gaëlle Geffroy, Ecole des Mines de Paris, France.

Abstract: After a functional definition of DRM systems (DRMs), this article studies the economic mechanisms of their roll-out over Internet networks. We underline the difficulty of their adoption by the vertical media chain (equipment and networks industries) on two-way communication networks compared to traditional one-way networks. We then analyze the overall competition between broadcast, physical, free and DRMs-based Internet distribution of digital contents.

Keywords: economic analysis – business models, competition, consumer behaviour, content protection, copyright law, stakeholders, standards

Introduction

This article stems from a study on the economic analysis of DRMs (Bomsel and Geffroy 2004) carried out within the FP6 IST project MediaNet. The objective of this project is to remove the obstacles to end-to-end digital communications and content exchange, from content/service providers to customers and between persons. In the MediaNet open architecture model it is crucial to examine the conditions under which Digital Rights Management systems could emerge and be reliable enough to ensure the compatibility of circulation of both copyrighted and non copyrighted material.

Digital Rights Management systems are means of assigning access to digital contents. This paper deals with the economic characteristics of DRMs. First, it aims at defining their economic functions, that is to say content *protection* and *versioning*. We then analyze the mechanisms of DRMs adoption over the Internet. Emphasis is put on the importance of network effects on complementary goods within dynamic vertical relations. We underline the difficulty of DRMs roll-out over two-way communication networks and draw the comparison with traditional one-way distribution networks. The final question is the overall competition between broadcast, physical, free and DRMs-based Internet distribution of digital contents.

DRMs: Protecting and versioning contents in the digital era

DRMs: Protecting contents in the digital era

The first goal of DRMs is to protect the exclusive rights of content owners. On the one hand – comparably to physical supports or entrance tickets – they exclude consumers from the consumption of the cultural good if they don't pay the price for it. On the other hand, they determine the range of uses granted to the consumers like other copying control mechanisms.

DRMs and all other private protection tools supplement copyright laws. Yet they follow different objectives. While private protection measures are designed to maximize rights owners' benefits, copyright law seeks for optimal social welfare. It therefore makes a trade-off between excludability, which provides incentives to creation, and the social benefits of diffusion. That is why the exclusive rights granted to the content owners are limited both in length and in scope by exemptions, like *fair use* and *first sale* doctrines.

Digitization has changed the terms of copyright laws' trade-off. By dramatically reducing the costs of copying, storing and transmitting digital files, it has increased diffusion possibilities together with threats to content owners' revenues and incentives to create. The DMCA (1998) and the EUCD (2001) made a relatively clear choice towards strengthening the ownership rules. While the first sale doctrine or principle of exhaustion cannot apply to digital files, anti-circumvention rules enable DRMs to override the traditional *fair use* limitations of copyright laws.

DRMs: Versioning contents in the digital era

The second function of DRMs is the versioning of contents. Contents address markets through a form of price discrimination called quality pricing or versioning. The idea is to

offer different qualities of the good at different prices to get consumers select themselves from among these versions, according to their different willingness to pay. Think, for instance, of hardback and paperback versions of a good.

DRMs enable content owners to make further versions of a digital file with respect to the liberalities of uses attached to it. They allow copyright owners to charge a price that varies according to the particular uses authorized. To be more concrete, digital files with embedded DRMs may offer various rights to modify or excerpt, time of possession, number of accesses, of copies on different devices or of people one can share with.

DRMs' enhanced versioning possibilities not only mean that content owners will better extract consumers' willingness to pay and increase their profits. Although it seems at first unfair to make people pay different prices, it may improve consumers' overall welfare. By enlarging the range of prices, versioning can allow more people to access the good, more consumers to be served. For instance, if audio digital file versions with restricted uses are sold at far lower prices than digital files with more liberal uses or than physical supports, new consumers may be able to enjoy songs.

DRMs roll-out and distribution networks competition

DRMs, network effects and standardization

Contents can't be taken apart from their distribution networks and encryption standards have to be accepted by the entire vertical media chain.

Networks effects are attached to products for which users' benefits increase with the number of users. Rolfs (1974) showed that there is a critical mass of subscribers below which a network cannot be sustainable. Once it is reached, every new consumer brings additional utility to all the others and the roll-out speeds up. A general rule to reach the critical mass is to subsidize the early adopters.

Distribution networks roll-out may be subsidized by piracy or circumvention of copyrighted media contents: the utility of the distribution industry is increased by the availability of free contents. This situation existed well before digitization. Yu (2003) and Varian (2004) refer both to the American delay of the International Copyright Act in the 19th century, that enabled the expansion of the domestic publishing industry thanks to pirated English novels until the rise of domestic authors at the end of the century (Hawthorne, Poe, Twain, etc.). As for content owners, they need their content to be protected against circumvention and benefit from its compatibility with the largest range of equipment. They have to make equipment and delivery networks industries accept a protection standard. But it is a different burden in two-way communication networks and in traditional one-way distribution ones.

In the case of one-way networks, like physical or broadcast distribution, content owners control the availability of contents and the indirect network effects. Equipment manufacturers have to accept their protection standard. An illustration of this idea is the recent broadcast flag agreement for the US over-the-air digital TV.

Over two-way communication networks like the Internet, everyone can technically broadcast contents. Moreover, circumvented contents are made available by individuals and not by professional pirates that could be located and prosecuted relatively easily. These contents are widely compatible thanks to free encoding formats like MP3 or DivX. As of today, the broadband Internet roll-out is largely subsidized by circumvented contents available through P2P applications. Circumvention benefits all complementary equipment as PCs, microprocessors, operating systems, printers, Internet modems, media players… . While DRMs oppose these Internet network effects, equipment and networks industries are not enforced to accept any encryption standard.

Nevertheless, some actors consider that DRMs roll-out is likely to happen in the future and are positioning themselves to have their proprietary solution accepted as the standard. That is for instance the game of Microsoft, Apple and Sony in the digital music market. This game results in a standards war bringing incompatibility between

DRMs. It delays DRMs adoption by consumers and extends over time the cross-subsidy of equipment and networks through copyright circumvention.

DRMs and the overall competition between distribution networks

The standards war on DRMs penalizes *legal* digital content distribution over the Internet and therefore benefits alternative diffusion systems: circumvention through P2P sharing, broadcast on dedicated networks and physical distribution. The overall competition between these different distribution networks depends also on price, quality, novelty and liberalities of uses.

- Physical versions could last for more than forecasted. They can increase their utility through quality and information density, decrease its prices or innovate in distribution like in the Netflix model (online DVD rental choice combined with postal delivery and return). Finally it can benefit from a valuable equipment legacy (the large base of DVD players).
- Content owners should push dedicated distribution networks like television or mobile phones. From an economic perspective, mobile phones are very comparable to broadcast networks because they distribute communication services according to a pay-for-service model. These distribution networks benefit from a stronger content protection and are easier to standardize. They could therefore benefit durably from a larger range of contents
- As for free contents on P2P networks, their total liberty of use contrasts with DRMs-files opaque restrictions and the advantage of DRMs-files is not systematic on quality and novelty. The on-going circumvention dynamics may have irreversible effects on broadband pricing and equipment. Being used to pay for capacity only (storage, processing, bandwidth) and to get always more value for his money, the broadband consumer may be reluctant to pay for services or contents. This behaviour may orient future investment in broadband networks.

Bottom line

DRMs are necessary to bring exclusion to digital IP goods. They are the only means to enable the exclusiveness of intellectual property rights and consequently, the sufficient incentives to create. While they restrict the short term consumers' benefits of cultural goods free diffusion, they insure their long term welfare by enabling these cultural goods to be financed and produced in the future.

The success and the pace of DRMs adoption will determine the format of the future digital libraries, whether encrypted or not. Two kinds of networks are presently competing to diffuse digital contents. One, the descending distribution model, in which the content owner masters the utility of the network, is DRM friendly. The other, the Internet open communication network, carries major circumvention incentives. A crucial stake in this competition is the roll-out of the home network equipment, i.e. the investment made by the consumer to equip his home with connected digital devices. This process will be shaping the access, the uses and the willingness-to-pay of the consumer for contents.

Sources

- Bomsel, Olivier and Geffroy, Anne Gaëlle (2004): Economic Analysis of DRMs. IST-Project: FP6-507452. Deliverable DB.5.14; http://www.cerna.ensmp.fr/Documents/OB-AGG-EtudeDRM.pdf
- Bomsel, O; Le Blanc, G.; Charbonnel, J.; Zakaria, A. (2004): Economic issues of content distribution. Cerna, Ecole des Mines
- DMCA (1998): Digital Millennium Copyright Act; http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html
- EUCD (2001): European Copyright Directive; http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf
- Fisher, William W. III (2004): iTunes: How copyright, contract, and technology shape the business of digital media – A case study. Digital Media Project. Berkman Harvard Law School
- MediaNet: Homepage of the project is at http://www.ist-ipmedianet.org/home.html
- Rohlfs, J. (1974): A theory of interdependent demand for a communications service. Bell Journal of Economics 5 (Spring): 16-35

- Varian, Hal R. (1997): Versioning information goods. (1998): Markets for information goods. (2003): The social cost of sharing. (2004): Copying and copyright. All papers are available at: http://www.sims.berkeley.edu/~hal/people/hal/papers.html
- Yu, Peter K. (2003): The copyright divide. Michigan State University

About the authors: *Olivier Bomsel* is senior researcher and professor of industrial economics at CERNA, Ecole des Mines de Paris. Contact: bomsel@ensmp.fr.

Anne-Gaëlle Geffroy is Ph.D. Student on the economics of digital contents at CERNA, Ecole des Mines de Paris. She works currently on digital copyright and vertical contracting issues in the media chain. Contact: ageffroy@ensmp.fr

Status: first posted 09/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=84

Violation of consumer rights with DRM-based usage control systems – The case of Half-Life 2

By: Danny Vogeley, Berlecon Research, Berlin, Germany

Abstract: DRMs for computer games was just about copy protection for a long while and it wasn't a hot topic. This is about to change with the Internet enabling DRM-based online usage control systems. The case of Half-Life 2 illustrates the potential of this approach and how it can be abused to violate consumer rights. Even though most players are heavily complaining about the usage control system, most of them do not forgo to play Half-Life 2.

Keywords: technical analysis – access control, consumer rights, content protection, DRMS, games, transparency

Introduction

Discussions about DRM usually focus on digital music or movies. The game market is often neglected in these discussions, despite its rising market size and the increasing relevance of DRM for the game industry.

In the USA 2001, the market volume of the game industry (9,4 billion Dollars) exceeded for the first time the turnover of the movie industry (8,1 billion Dollars) (Wirtz 2003, p. 493). The production and marketing costs of high quality games such as "Lord Of The Rings – The Two Towers" by market leader Electronic Arts was above 25 million Dollars (Jensen 2003, p. 49). Successful games like Myst have realized revenues of 125 million Dollars (Wirtz 2003, p. 493). It is estimated that the turnover of the PC and video game market worldwide is about 18,8 billion Euros (VUD 2005).

Rising importance of DRM in the game market

Piracy and the emergence of new DRM-based business models are a big issue in the game industry as well. National entertainment software associations worldwide like the British ELSPA (www.elspa.com) or the German VUD (www.vud.de) are complaining about massive sales losses due to illegal circulation of game copies. For example, it is estimated that in Germany about 11 million blank CDs/DVDs have been illegally used to burn copies of games between January and June 2004 (GfK 2004).

Therefore, the most important role of DRM in the traditional gaming market has been pure copy protection for CDs and DVDs. But other roles of DRM are gaining more and more importance. Similar to the digital music and movie market, DRM systems are now more frequently deployed to enable new online distribution (streaming, full-download) or revenue models (subscription services, pay per game/time).

In addition, new roles that are rather unique to the game market are gaining significance. Examples are the management of the game play and persistent online usage control. The

management of game play relates to the control of a played game itself. For example, in multiplayer online role games, the developer is in charge to supervise a virtual world. Among other things, a developer prevents cheating among role players or controls the trade of virtual assets. Virtual assets, such as valuable weapons or virtual money, have often been traded on eBay without the permission of the game developer. Therefore, DRM can be implemented in virtual assets to control or restrict such trading.

Online usage control encompasses the management of access to and further usage of retail games via the Internet. Retail games are sold in CD or DVD boxes, which are usually played in offline modus on PCs. Traditional access control mechanisms of retail games are focused on a closed system environment: When the copy protection of a game has been cracked or a license number is shared, it can be easily disseminated to other systems beyond the developer's control. However, the Internet has enabled new control mechanisms, which have the potential to manage the access and further use of a game persistently. They can be considered as DRM technology, because they give a content distributor a sophisticated means to manage game users' rights persistently. Persistent usage control mechanisms have a special potential on the game market, because for game players there exist incentives to uphold an online relationship with the game developer. Unlike music or movies, games themselves are highly adaptable and can be enriched with additional features like new game levels, maps or weapons. There is a high demand for such features for an enhanced and continuous game play.

Online usage control systems force the purchaser of a retail game to validate it via the developer's online platform. If a developer assumes an illegal use, he may disable an account instantly. Game access activation can be required only once during game installation or repeatedly over a given period. The latter gives the game provider an ongoing control system to identify illegal licenses. Although a user might have successfully registered an unlicensed copy of a game at the initial activation process, he cannot be sure if this illegal license will not be detected the next time. As a result, to crack a game only once will not be sufficient any more. This is especially efficient against the casual user, who often receives cracked games or licenses from friends.

Case Study: Half-Life 2

The first game developer to use DRM as an online usage control system for retail games is Valve. Valve uses its online platform "Steam" as a Digital Rights Management system to verify legitimate access keys and to keep control of the further usage of its games. Steam is also deployed to administer customer billing, to provide updates and to allow the users to backup games on CD-Rs or DVD-Rs. Valve introduced Steam as a DRM system with the release of Half-Life 2 in October 2004. Half-Life 2 is a so-called first-person shooter game, in which the user basically takes a first-person perspective in a three-dimensional space to battle against enemies. It also provides the option to play it in a multi-player mode. Half-Life 2 is a long-awaited sequel to Half-Life in the game community. Its production time was several years.

To install Half-Life 2, Valve requires in addition to an online activation the creation of a personalized online account via Steam. If Steam detects any identical licenses, it will cancel all accounts that have used these licenses. Steam even disables the account of the user that originally obtained the license legally. Valve claims to have cancelled more than 50.000 (allegedly) illegal accounts so far.

Beyond the pure authorization of legally obtained games, Valve's Steam also has the potential to intensively control the user. For example, Steam has been abused to postpone the point in time when users were able to start playing Half-Life 2. After the official release of Half-Live 2 in November 2004, purchasers were not able to install and play their games for almost one week. Valve had been in a contractual licensing dispute with its distributor Vivendi, which did not allow Valve to unlock Half-Life 2 during this legal issue. In this case, the purchasers of Half-Life 2 were locked in a licensing battle be-

tween two corporations (Grimmelmann 2003).

The relevance of usage control systems will gain significance, when they are used to enforce changes to an End User License Agreement (EULA). For example, Valve reserves the right to change fees or billing methods at any time. Therefore they force users to agree to review the EULA periodically for any amendments:

> *"Valve reserves the right to change (...) fees or billing methods at any time and Valve will provide notice of any such change in at least thirty (30) days advance. All changes will be posted as amendments to this Agreement or in the Rules of Use and you are responsible for reviewing the billing section of Steam to obtain timely notice of such changes."*
>
> *"Your non-cancellation of your Account thirty (30) days after posting of the changes on Steam means that you accept such changes."* (Steam 2005, section 4b)

In other words, Valve basically allows its customers to use their game only as long as Valve wants them to have it. Valve claims the right to demand additional fees at any time without notifying its customers personally. When a user connects to Steam to receive additional features or necessary patches, which are normally provided for free, he cannot be sure if he will not be billed. With Steam, any changes in the EULA will affect the game user instantly. Regardless of whether Valve has the legal right or not to disable accounts, Valve can simply do it. And if one considers going to court, it is especially difficult for non-US citizens to sue this US-based company for any unfair practice. With Steam in combination with its EULA, Valve can be described as judge, jury and executioner.

In another section of the EULA, Valve claims the right to download via Steam additional software or updates on users' computers without noticing them:

> *"Steam and your Subscription(s) require (...) the automatic download of software, other content and updates thereto onto your computer. (...) You understand that Steam may automatically update, pre-load, create new versions or otherwise enhance the Steam Software and accordingly, the system requirements to use the Steam Software may change over time."* (Steam 2005, section 2b)

Users of Half-Life 2 have to agree that Valve is going to download software beyond the users' control, when they connect to Steam. This can be convenient to keep the game up-to-date automatically. But the consumers do not have the choice whether they are going to allow it or not. This lack of control is especially critical, because Valve does not guarantee that the downloads will be virus-free or secure (Steam 2005, section 9b).

Even though playing the game does not require a connection to Steam after the initial activation process, the default setting of Half-Life 2 automatically establishes an online connection to Half-Life 2. Many game players are not aware of the possibility to play this game in offline mode and changing the default settings is rather complicated. The documentation about this function is limited.

How do the consumers react?

However, Valve's online usage control system and its restrictive EULA did not result in low sales of the game. Quite the opposite can be observed: Between November 2004 and January 2005 Half-Life 2 has been sold more than 1.7 million times. Currently it is still one of the best sold games worldwide.

Looking at different game forums on Half-Life 2, the online activation via Steam and the continuous binding to this online platform is by far the most discussed topic. But although there are mostly massive complaints about Valve's rigid usage control system, most of the players would not forgo buying the game. In contrast, there are hardly any extensive discussions on how DRM systems might enforce amendments to the End User License Agreement. Therefore it can be assumed that most users of Half-Life 2 are not aware of the content of the EULA. Often users of games or other software products do not read EULAs. EULAs are considered too long and incomprehensible. Above that, Valve's EULA is only available in English, which is a hurdle for many non-English speakers. It can be assumed that most users are not aware of how amendments in the EULA can be enforced by Steam. Game

players have so far no experience with this kind of extensive user control.

This case is also about transparency. Recently the Federation of German Consumer Organisations (VZBV) sent a cease and desist order to Valve and its distributor Vivendi, complaining about their insufficient DRM information policy. The term "Internet connection" as a requirement is merely listed in the "other" category on retail boxes. The need for online activation is not clearly indicated. Because the EULA is only available in English and cannot be read before the purchase it raises the question, whether it is at all legally valid. However, Steam is still in use and controls 1.7 million customer accounts at its will with its DRM.

Bottom line

DRM-based usage control systems can be abused to violate consumer rights. It is alarming to see how little consumers have reacted to this practice and that it has not negatively affected sales of the game. This could pose an incentive for other developers on the game market to use online usage control system to restrict consumers' rights. DRMs developments on the game market, therefore, have to be closely watched in the future.

Sources

- GfK (2004): Piracy-Study 3. Gesellschaft für Kosumforschung, Nürnberg, Germany; http://www.ffa.de/start/download.php?file=publikationen/brenner_studie3_en.pdf
- Grimmelmann, James (2004): Two Skirmishes in the DRM Wars: Half-Life 2 and Halo 2. Yale Law School's LawMemeEST, Nov. the 14th; http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1647
- Harris, Wil (2005): Is the Half-Life 2 EULA illegal? In: The Inquirer, 05-02-06; http://www.theinquirer.net/?article=21105
- Jeges, Ernö (2004): Turning infringing users into paying customers - A new trend in anti-piracy. INDICARE Monitor Vol. 1, No 6/7, 17 December 2004; http://www.indicare.org/tiki-read_article.php?articleId=64
- Jensen, Lars (2003): Das Spiel geht weiter. In: Brand Eins, No 4, Berlin, pp. 46 – 50
- Newitz, Annalee (2005): Dangerous Terms - A User's Guide to EULAs. The Electronic Frontier Foundation; http://eff.org/wp/eula.php
- Steam (2005): STEAM SUBSCRIBER AGREEMENT; http://www.steampowered.com/index.php?area=subscriber_agreement
- VUD (2005): Computerspiele als Wirtschaftsfaktor. Verband der Unterhaltungssoftware Deutschland e.V. Paderborn, Germany; http://www.vud.de
- Wikipedia: Half-Life 2: http://en.wikipedia.org/wiki/Half-life_2
- Wikipedia: Steam: http://en.wikipedia.org/wiki/Steam_%28content_delivery%29
- Wirtz, Bernd (2003): Medien- und Internetmanagement. Wiesbaden, Germany

About the author: *Danny Vogeley* is an intern at Berlecon Research. He has been analysing several digital markets like Internet broadcasting, mobile music and M-Business strategies of media companies. Currently, he works in the field "digital consumer". He is a member of the INDICARE project team.

Status: first posted 10/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=85

How to implement copyright exceptions in DRM systems

A proposal substantiated for the copyright exceptions in German law

By: Dominik Knopf, Institute of Information Law, Karlsruhe, Germany

Abstract: This article is based on a diploma thesis (Knopf 2004) in "information engineering and management", which has been submitted to Prof. Thomas Dreier at the University of Karlsruhe. Copyright exceptions and DRM systems (DRMs) normally do not interact very well. The approach presented in this article describes a way to achieve a win-win situation for both - consumers interested in copyright exceptions and content providers wishing to protect their content -, by implementing the exceptions demanded by law directly in the DRMs. Benefits are a higher level of trust and an extended global protection of the content, because the content never leaves the protection of the DRMs.

Keywords: technical analysis – copyright law, DRMS design, fair use, private copy

Introduction

Currently DRMs are yet unable to reconcile the conflict between rightsholders' interests and public access interests. They restrict use possibilities and thus curtail the freedom granted to users under exceptions to the exclusive rights of copyright holders. Not surprisingly, consumers have begun to develop distrust to any new invention regarding content and rights management.

So how can trust be regained? To begin with, consumers must be assured that their personal data are as safe as they would be in a normal store in the "real" world. Only very few consumers would supply information on how often and when they hear a piece of music. In addition, there is more personal and private information at stake, e.g. information about a handicap someone has. Next consumers will not accept a new system if they feel unnecessarily intruded, i.e. if they are limited to freely use content once they have bought it. Thirdly the ability of DRMs to override legal provision, in particular the exceptions granted, creates further distrust. Obviously there is no easy solution to implement DRMs fulfilling these consumer requirements.

The approach outlined here starts from a paradigm shift: from object-oriented DRMs to user-specific DRMs. It is proposed to link the content to the person, who acquired the rights to use the content, and not to the object the content is used with. Due to this switch in perspective, the implementation of copyright exceptions becomes possible.

The main elements of the approach

Trusted third parties

This approach is based on an infrastructure which includes a set of trusted third parties (TTP). These TTPs work as mediators between the consumers and the companies. Their tasks are:

- anonymization of the consumers' data
- bearing witness to the consumers' characteristics regarding copyright exceptions (e.g. "person A is a student")

To guarantee the TTPs' impartiality, TTPs should be state-run or they should be run by an independent commission. Exactly which TTP is chosen depends on the particular exception.

Dongle for identification

The second part of the infrastructure would be a safe way to identify the consumer sitting in front of the computer. A system which could work well would be a combination of a computer dongle as a physical component (e.g. an USB device with cryptographic capabilities) and a personal code to access the private key on the dongle. Every dongle is unique and can essentially not be copied.

Technical Protection Measures (TPM) / watermarks

It should be noted that watermarks – as a safe way for linking content to the consumer – are

also an essential part of the user specific DRMs. Watermarks fulfil an important function in this approach. It is assumed that watermarks can be integrated in every format the consumer wants to use, even in already existing standard data formats. Watermarks are the essential way to maintain the link between the consumer and the content he controls.

How it could work for different kinds of exceptions

The concept outlined above will be demonstrated by the following three examples. The first of these examples describes its realization with respect to § 45a UrhG. This exception was introduced into the German Copyright Act in order to protect the access to information for handicapped people. The second example describes the implementation of § 52a UrhG which protects the access to content for scientific use and use in teaching. The third example is about the implementation of the much discussed private copy exception contained in § 53 UrhG. Ideally all examples described will become fully automated.

Implementation of § 45 UrhG (exception for disabled people)

For this scenario a public office should be chosen as TTP, which has already access to information regarding the degree and the kind of the handicap of the consumer. Consumers, who fall under this exception normally buy content and contact the TTP afterwards and supply a certificate of the content provider which proves that they bought the rights to use the content. The TTP verifies this certificate and asks the content owner for a copy of the content, which can be used by the consumer. The copy gets personalized to a new ID and is resent to the TTP, which also resends it to the consumer. The consumer can now use the content. In the case of a copyright infringement, the TTP has a connection between the new ID and the personal data of the consumer.

Implementation of § 52a UrhG (exception for scientific use and the use in teaching)

Other TTPs are universities and comparable institutions, which have access to information regarding students, teachers and lessons held. Students are required to register for lectures at the TTP to minimize the efforts for the participants. The teacher giving the lecture registers all relevant content at the TTP. When a student needs access to content, he contacts the TTP, which then contacts the content owner. The procedure then follows the steps as set out with regard to the implementation of § 45 UrhG.

A second way of implementation is to add the watermark of the student – if he has one – to the watermarked version of the professor. This can be done by the DRM-application itself and there would be no need for a TTP. So, students presumably would not distribute their copy with their personal data in the watermark.

Implementation of § 53 UrhG (exception regarding the private copy)

This implementation of the private copying exception is a little bit more sophisticated. Before even implementing this exception, a preliminary question has to be asked: Why should this exception get implemented at all? Well, users have become accustomed to making copies of the copyrighted material they have bought or accessed for purposes of time and place shifting, for format change and also for archiving and security reasons. By implementing the private copy directly in the DRMs, a private copy continues to be possible for the consumers and is used more reasonably.

In general, consumers obtain the data protected by DRM over the internet or in a store. In the first case, in the model proposed, data gets marked with a personalized watermark at the moment of the sale. In the second case, data gets personalized when it is used for the first time. When a consumer would like to copy his data within the limits of the private copying exception, depending of the use of the data, the consumer uses his or her DRMs to generate a copy, which supports the intended use. For example, if the user wants to hear a song in a DRM-protected format on his MP3-player, his DRM-application converts the data, embeds a watermark and copies it on the MP3-players, tagging it in such a way that it can't get copied back. If the MP3-player already supports a proprietary DRMs,

the application should be able to convert the data to this format.

A way to use the internet in the last scenario could again involve a TTP, which requests a DRM-protected, newly watermarked copy of the content from the content owner. Consequently there is no need to change watermarks.

For the consumer, the private copy still exists, but in the case of copyright infringement, his name or ID is on the copy. This will limit the consumer's interest in distributing the content. But the consumer is still able to use his content like he was used to, when it wasn't DRM-protected.

Discussion

As with all DRM-approaches, there are some advantages and some disadvantages. The most evident problem of the present proposal is the creation of the infrastructure. The implementation will only be affordable if there is a standard system which is usable for a broad variety of services. Most likely the infrastructure required has to make use of other infrastructures being build up, e.g. the infrastructure for the German health system relying on a health card (Gesundheitskarte) with cryptographic abilities. However, if a combined system can be violated, the damage would be much greater. Therefore a safeguard has to be available.

A second problem is the dongle. The dongle provides more security for the content owner and makes content mobile for the consumer, but it is also a cost factor. Moreover, the consumers' comfort is somewhat limited by a dongle. It may generate technical problems and consumers would have to attach it to the computer every time they want to use their data.

A third and minor problem is the fact that under the model proposed, the TTP gets information about consumers' access to the services of the content owner. Therefore it must be ensured that the TTP adheres to data protection and privacy policies.

Finally, there is a problem that all DRMs have in common: The system works only as long as cryptographic security (including watermarks) can be warranted and if consumers use the system in a responsible way. But if, e.g. a dongle gets lost, this will be like losing a credit card. This, users will have to understand.

However, as already mentioned in the introduction, there are also some positive elements in this approach, which compensate for the negative ones.

First of all, because of the effort which the content owner undertakes with such a system, he demonstrates that he does not really want to limit the rights of the consumer any further than defined by statutory provisions. This brings at least some credibility back and should increase the trust on the part of the consumers. A certification of such a DRM system could further increase this effect. Also, consumers' personal data regarding handicaps or relationships between consumers remain safe at the TTPs. Finally the content owner can be sure that his content never leaves the protected circle even if private copying is allowed.

While it is doubtful, that the system will be implemented very soon due to the high cost factor, it may be an option in the near future, when an identification infrastructure exists. As more and more people, companies and public offices are relying on the new digital technologies, the cost of adding TTP-capabilities in an office or a commission will be reduced. It is also imaginable that future laws will *require* the implementation of copyright exceptions in DRMs as a prerequisite to the granting of legal protection.

While this approach has been discussed with respect to the German copyright exceptions, it is possible to use it with minor changes for other national transpositions of the European copyright directive too.

Bottom line

Intellectual property entails rights and responsibilities. At the moment code tends to substitute law. Therefore, code – in this case code of DRMs – cannot stay uncontrolled. There will be a control instance, either by law or by self-regulation. The approach presented here can be a way to allow for a well-balanced technical regulation. The paradigm

shift proposed should help to represent the law more correctly, because the law in fact links rights to persons and not to objects. Any technology should enable consumers to enjoy their rights on whichever device they like. DRMs are a great opportunity to solve the problem of intellectual property if it is used right. But it must work for both sides. Due to today's (dis)abilities of TPMs, the natural way of using the content is blocked.

Sources

- German Copyright Act; http://bundesrecht.juris.de/bundesrecht/urhg/
- German "Gesundheitskarte" (health card); http://www.bmgs.bund.de/deu/gra/themen/gesundheit/geskarte/index.cfm
- Knopf, Dominik (2004): Diploma Thesis (unpublished): Durchsetzung rechtlich geschützter Zugangsinteressen durch nutzergruppenspezifisches Digital Rights Management (Enforcement of the legitimate interest for access via user group specific Digital Rights Management); http://www.dknopf.de/papers/diploma%20thesis.pdf

About the author: *Dominik Knopf* finished his studies in information engineering and management at the University of Karlsruhe by the end of 2004. Currently he is working with Prof. Thomas Dreier at the Institute of Information Law at the University of Karlsruhe, and is preparing his doctoral thesis.

Status: first posted 21/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=87

Comparing the EUCD implementation of various Member States

Reviewed publication: Urs Gasser and Michael Girsberger, Transposing the copyright directive: Legal protection of technological measures in EU Member States. Cambridge, MA: Berkman Center for Internet & Society Research Publication Series (no 2004-10), November 2004

By: Margreet Groenenboom, IViR, Amsterdam, The Netherlands

Abstract: The paper reviewed analyses how the EU Member States have implemented the anti-circumvention rules provided for in the European Copyright Directive (EUCD). It focuses on three main issues: (1) definitions, (2) the relationship between the protection of technological measures and exceptions to copyright as described in Article 6 of the EUCD, and (3) sanctions and remedies according to Article 8 of the EUCD. The review compiles the main findings of the excellent paper giving rise to only minor points of criticism.

Keywords: review, legal analysis, policy analysis – EUCD, content protection – EU

Introduction

In November 2004 two affiliates of the Berkman Center for Internet & Society, *Urs Gasser* and *Michael Girsberger*, published a research paper on the transposition of the Articles on technological protection measures (TPM) of the European Copyright Directive (EUCD) by various European Union Member States (Member States). In particular it gives an overview of the current state of implementation of Article 6 (circumvention of TPM) and Article 8 (sanctions and remedies) EUCD. Countries that had already implemented the EUCD in the last quarter of 2004 were: Austria, Denmark, Germany, Greece, Hungary, Ireland, Italy, Luxemburg, Malta, The Netherlands, Poland, Slovak Republic, Slovenia and the United Kingdom. The aim of the report is neither to describe every single country nor to come up with a critical assessment of all approaches taken, but to present a representative selection of interesting models and to take a critical look at the level of harmonization reached in the Member States.

The report consists of three parts: *Part one,* "how the Genie got in the bottle", describes the history of the EUCD and the current state of implementation of the EUCD. *Part two*, "Overview of Article 6 and Article 8 EUCD", describes the subject matters that the report investigates. *Part three*, "Country-specific analysis", describes the implementation of the EUCD per subject matter in several Member States.

In this review, the first two parts of the report are introduced briefly. As part three is the one where it all comes to a head, most attention is paid to this part.

Part 1: How the Genie got in the bottle

The report goes back to the adoption of the WIPO Copyright Treaty (WCT) in 1996 and to the WIPO Performances and Phonograms Treaty (WPPT). Very relevantly, the report observes that already in the Articles 11 WCT and 18 WPPT, the provisions that deal with the circumvention of TPMs, do not define the terms "effective" and "technological measures". Was this the moment where it already went wrong? In my opinion the lack of definitions allowed for rather different approaches, the major ones being the DMCA (1998) and the EUCD (2001). This part also describes the current state of implementation of the EUCD. Since several countries still have not implemented the Directive and are thus still struggling with it, the report concludes saying that "the Genie is stuck in the bottle".

Part 2: Overview of the Articles 6 and 8 EUCD

The second part forms the necessary basis for the country specific analysis in the third part. It describes the Articles 6 (TPM) and 8 (sanctions) of the EUCD focussing on (a) definitions, (b) the relationship between TPMs and exceptions to copyright law, and (c) sanctions & remedies.

(a) Questioning the definitions of the EUCD
Article 6 EUCD protects TPM against circumvention and against the trafficking of circumvention devices and services.

When describing Article 6 (3) (the devices), attention is paid to the lack of an explicit distinction between "access control" and "copy control" devices. Where Article 6 (3) mentions "through application of an access control or protection process such as encryption, scrambling" this leads according to the report to "the presumption that the EUCD does analytically distinguish between access and copy controls but – unlike the DMCA – grants equal treatment to both types of technology". The report mentions later (page 13) that §1201 of the DMCA makes this distinction. Indeed, the distinction between "*access control"* (measures that effectively control access to a copyrighted work) and "*copy control"* (measures that effectively protect a right of a copyright owner) is essential in the United States (see DMCA § 1201; see also Reese 2003).

Circumvention (§ 1201 (a) (1) (A) DMCA) as well as *trafficking* in circumvention devices (§ 1201 (a) (2) DMCA) is not allowed with regard to **access control mechanisms**. In this case, civil remedies and criminal provisions under § 1203 and § 1204 DMCA are possible. It is *not* forbidden to *circumvent* **copy controls**. *Trafficking* in circumvention devices with regard to copy controls is forbidden and is subject to the provisions § 1203 and § 1204 DMCA (§ 1201 (b) (A) DMCA). Although *circumvention* of copy controls is not forbidden, remedies are still possible for copyright owners. The *circumvention* of copy controls can still lead to liability for copyright infringement under § 501(a) DMCA because an unlawful reproduction or distribution might have taken place, but this depends on what is done by the circumventor after the circumvention.

(b) Protection of technological measures and exceptions to copyright
Member States have to take appropriate measures to make sure that it is possible for beneficiaries to benefit from the exceptions that are applicable to the exclusive right of the copyright owner (see also Helberger et al 2004, p.49). The report identifies two main categories of exceptions:

- Public policy exceptions (such as exceptions in relation to photocopying, copy and archive purposes of educational facilities). Although these exceptions are

mandatory, recital 51 EUCD states that appropriate measures should only be taken in absence of voluntary measures taken by rightholders, including the conclusion and implementation of agreements between rightholders and other parties.

- Private copying exception. In this case Member States may, but are not obliged to take measures to make sure that people are able to make a copy for private use.

The public policy exception as well as the private copying exception do not apply to on-demand services. On demand services are defined in article 6 (4) as "works made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them". What "appropriate measures" are or can include, is not specified by the EUCD.

(c) Sanctions and remedies (Article 8 EUCD)
Important here, is that Member States are obliged to "provide appropriate sanctions and remedies", to "take all the measures necessary to ensure that those sanctions and remedies are applied" and "sanctions have to be effective, proportionate and dissuasive".

Part 3: Country specific analysis

The report describes the implementations of the Articles 6 and 8 EUCD by several Member States. The three aspects introduced in the second part in a general way are used her e again for the country comparison. The report convincingly shows the difference of national approaches when implementing the EUCD in Member States.

Unfortunately it is not clear what criteria were used to select the countries that are described per subject matter. Sometimes a country is mentioned only in relation to one aspect (Austria, Ireland, Hungary and Italy), sometimes to two (Greece and the Netherlands), and sometimes in relation to all three aspects (Germany, Denmark and the UK). In this review, only countries that have been described for that particular subject matter are mentioned.

(a) Problems related to the definition of TPM
The report perfectly clarifies why definitions are very important. As an example, region coding of a DVD is used. In practice, two main approaches exist in the area of what acts the EUCD prohibits:

1. Only TPMs that prevent or restrain uses that are relevant under the copyright law and that would result in copyrights infringements are protected. This is called the *narrow interpretation*.

2. TPMs aimed at preventing or restricting *any* act are protected. This is the *broad interpretation*. In this scenario there is no connection with the acts that are relevant under copyright law. A connection is made with "the acts that are not authorized by the rightholder". Thus, the acts that are not authorized by the rightholder, are protected against circumvention.

Hungary and Denmark are examples for the *narrow* interpretation of the definition of TPM. The Danish Act is applicable to TPMs "that are designed to protect works from copying" and the act *excludes* mere access controls from the protection because access control technologies do not necessarily prevent an act that would constitute an infringement by copyright law. This approach is quite interesting because if a user circumvents a TPM solely to make use of a lawfully acquired work (for instance: breaking the region code of a lawfully acquired DVD to play it on the computer), this circumvention is allowed.

Other countries, like Germany, the UK, and the Netherlands, adopted the *broad* interpretation. Consequently, in these countries control mechanisms can be protected against circumvention even if the mechanisms are not designed to prevent exclusively acts that are relevant under copyright law.

(b) TPM and exceptions to copyright, Article 6(4) EUCD
With regard to the exceptions to copyright, there are major differences between Member States. I will have a look at the private copying exception, the public policy exception, what if voluntary measures fail and finally at the definition of "on demand services".

► Private copying exception?

The approach to the private copying exception is different among Member States. In Denmark private copying is not mentioned at all. In the UK the act expressively refers to "time-shifting" as the only private copying exception permitted and in Greece only reproduction for private use on paper or any similar medium is mentioned. In Italy it is possible to make one copy for personal use provided that a) the user has obtained legal access to the work and b) the act neither conflicts with the normal exploitation of the work nor unreasonably prejudices the legitimate interests of the rightholder.

► Public policy exceptions?

In Ireland and Greece, rightholders should make available means to beneficiaries to benefit from the exceptions. The Austrian and the Dutch approach is the wait and see strategy (using recital 51 EUCD) and therefore there are no exceptions to the anti-circumvention provision. In Austria a recently conducted survey shows that the voluntary measures taken by rightholders are in compliance with the EUCD (Bericht Bundesministerin für Justiz, 2004). Although there are problematic areas (i.e. access and copy protection technology on CDs and DVDs) no legislative measures have been announced.

► What if voluntary measures fail?

In case rightholders do not take voluntary measures or when the measures do not allow the use of an exemption in the eyes of the beneficiaries, it depends on the country which steps need to be taken by beneficiaries. Sometimes beneficiaries may apply directly to the Copyright License Tribunal (Denmark), High Court (Ireland) or Secretary of State (UK). In Denmark, when rightholders do not comply with the order within four weeks, beneficiaries may legally circumvent the TPM, as long as the consumer has gained legal access to the work. They don't need approval of the Tribunal or anyone else to do this. In other countries, like Greece, the solution is sought in mediation (with the possibility to go to Court of Appeal of Athens).

► On-demand service

What is noteworthy with regard to the exclusion of the "on demand services" from the applicability of Article 6 (4) par 1 and 2, is that the countries that implemented exceptions (Ireland, UK, Denmark and Greece), all use the exact sentence used in the EUCD to describe "on demand services" as "works made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them".

(c) Sanctions and remedies, Article 8 EUCD

The implementation of Article 8 is very diverse, in some countries huge criminal sanctions are possible (imprisonment or a fine of 2,900 – 15,000 Euro in Greece or 10,000 – 50,000 Euro in Germany), whilst in other countries there is no imprisonment and only a small fine (Denmark).

There is a difference in what acts can be subject to penalties. In the UK, there are no criminal sanctions for the circumvention of TPMs as long as it is conducted for private and non-commercial use. The UK also has a special Article in which is stated that the infringement that occurs in the course of business or "to an extent that prejudicially affects the rightholder" can be qualified as a criminal offence.

In Denmark, Greece and Germany, circumvention of TPMs as well as the trafficking in circumvention devices can be punished under civil and criminal law. Imprisonment for these acts in Denmark is not possible. In Greece imprisonment of at least one year is possible. Germany makes a distinction between the circumvention of TPMs (imprisonment up to one year or a fine) and the trafficking in circumvention devices (imprisonment up to three years in case of professional purposes or a fine). Remarkable is the fact that in Germany (similar to the UK) no criminal sanctions are applied in case the act has been exclusively performed for, or in relation, to private use by the offender or individuals personally connected with him.

Conclusions of the report

The report ends with two concluding remarks. First of all, the report draws the con-

clusion that the Member States are still struggling "with some problems already identified at the level of the EUCD, such as the definition of TPMs, scope of protection and the interface to exceptions, and the question of effective , but also adequate sanctions and remedies". Most countries leave it to the national courts and the European Court of Justice to "fine tune the new legislation".

Secondly, the authors conclude that although the EUCD has led to a certain level of harmonization, significant differences remain. Also, it remains to be seen what the ramifications of these differences will be, for instance with regard to the further development of digital media markets, technological innovation, and the evolution of the "regulatory ecosystem".

A bit of discussion

Overall the report gives a good idea of how different some implementations work out when they are applied to the examples mentioned in the report. The comparison between the DMCA and the EUCD regarding the distinction between access and copy control is interesting and certainly deserves more research and discussion in Europe.

One point of criticism; the report notes in the section about the private copy exception, that Italy "might stand alone in this issue" because some recent court rulings in France, Belgium and Germany all decided against a "right to private copying". Against this opinion, one could argue that although there may not exist a right that consumers can enforce as consumer in court, this does not mean that the private copying exception ceases to exist.

Unfortunately (besides the fact that the selection criteria for the countries chosen are not explained) the consequence of working with a selection of countries is that it is not possible to make an overall schedule of which countries use a narrow approach, and which countries use a broad approach, or to make any profound aggregation at all of the implementations of the articles 6 and 8 EUCD, because the selected countries for the subject matters vary. An overall view of the implementations would be helpful when assessing the implementations of the articles 6 and 8 EUCD in the Member States.

Lastly, the issue of region coding mentioned by the report is quite interesting. How can region coding be qualified and what are the consequences of the qualification in combination with the approach of a Member State with regard to the definitions of TPM in the EUCD, i.e. does a country use a broad or a narrow definition. At the moment, the difference in treatment regarding region coding in different Member States does not result in harmonization of "a European approach" at all.

Bottom line

Overall, the report is very well written and easy to read for lawyers and non-lawyers. The report also draws an interesting picture of the implementation struggle and the diversity of implementation paths with respect to the focus chosen. Finally, it invites to further investigate the consequences of a narrow or a broad interpretation of what TPMs are protected by the EUCD.

Sources

- Gasser, Urs; Girsberger, Michael (2004): Transposing the copyright directive: Legal protection of technological measures in EU Member States. Cambridge, MA: Berkman Center for Internet & Society Research Publication Series (no 2004-10), November 2004, http://cyber.law.harvard.edu/publications
- Bundesministerin für Justiz, Bericht der Bundesministerin für Justiz im Einvernehmen mit dem Bundesministerium für soziale Sicherheit, Generationen und Konsumentenschutz an den Nationalrat betreffend die Nutzung freier Werknutzungen, July 1, 2004, available at http://www.justiz.gv.at/_cms_upload/_docs/bericht_freie_werknutzung.pdf
- DMCA (1998): Digital Millennium Copyright Act of 28 October 1998; http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html
- EUCD (2001): European Copyright Directive, http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf
- Helberger et al (2004): Helberger, Natali (ed.); Dufft, Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich: Digital rights management and consumer ac-

ceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report. Amsterdam; available at http://www.indicare.org/soareport

- Reese R. Anthony (2003): Legal Incentives for adopting Digital Rights Management Systems: Merging access controls and rights controls; available at https://www.law.berkeley.edu/institutes/bclt/drm/papers/reese-drm-btlj2003.pdf

About the author: *Margreet Groenenboom* is project researcher at the Institute for Information Law, University of Amsterdam. She specialises in copyright law, patent law and law & information technology. Contact: + 31 20 525 7382, groenenboom@jur.uva.nl

Status: first posted 21/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=88

Better take a long tail look...

Three remarks on the INDICARE state-of-the-art-report

By: Timo Ruikka, Nokia Corporation, Espoo, Finland

Abstract: The INDICARE report is regarded overall a good reading and highly useful. However three issues shall be highlighted where the author of this review disagrees with INDICARE and does propose a broader and longer term perspective of the changes we witness.

Keywords: review, INDICARE – business models, consumer expectations, innovation, privacy

New business models and flexibility offered by DRM

I found the issue of new business models and flexibility offered by DRM to be incompletely articulated in the report. I personally believe that there can be HUGE value to users in getting something less (in usage rights) than what the content industry is afraid to distribute in wide circulation (that being the freely copiable personal copy like the CD disk is today). If it is a good deal, users can accept something less than permanent and something that is less than freely transferable. This does assume that prices also come down from the early trial phase that we are witnessing now. In fact, I expect the prices to go down so far that users will consume content like they consume electricity: without thinking how much a minute costs but turning it off when finished – like they turn off lights when they go out.

Also, the flexibility will be in the incredible selection (see on this the Wired magazine article by *Chris Anderson* 2004 "The Long Tail") and in the tailoring to changing needs and tastes: having a constantly updated top 100 songs in your pocket is flexibility even if you cannot transfer any of those tracks to another device...

Now, if prices do not come down so far, then I trust the consumer advocates will make a big noise... .

Consumer expectations that really matter

Consumers do not really need detailed transparency, they do not want to dread the small print of what consumption possibilities are offered when they buy content online. Instead, they need simplicity and predictability of stable, balanced, well defined typical consumption offerings. In my view, the "small print" and the detailed scope of the typical offerings should be negotiated by all stakeholders. The result should be as familiar as a train ticket: you do not read the fine print when you buy one. But you have a pretty clear idea about the main variables: monthly pass, 2nd class return, 2nd class one way. Or all-you-can-eat Eurailpass etc! You get the idea. Now 3,000 service providers are inventing the same packages in s-l-i-g-h-t-l-y different ways and it will drive consumers crazy.

Against the myth that DRM is a privacy issue

Privacy is relevant for DRM-enabled services. But this concern is generic to all digital services, it is not DRM specific. The INDICARE paper has far too great emphasis on privacy aspects, as if DRM was a bigger threat to privacy than (for instance) eBay or electronic banking or credit card statements. The privacy aspect is whether a service accumulates personally identifiable information and how it handles that information. DRM per se does not generate PII (Personally Identifiable Information). Nor do DRM systems typically "track" users and what they do with the content – instead they just limit the functionality of content received by users. The main linkage DRM has to privacy is that it includes support for digital identities: Device identity, domain identity (e.g. a home of several devices) and even personal identity (if a person's name is linked to a subscription ID like an Internet username and PIN). But similar identities are in use in almost all Internet services. So let's not continue the myth that DRM necessarily is a privacy issue. Some SERVICE models can be BIG privacy issues (like TiVo which collects viewing habits and begins to suggest similar programs; Amazon does this too). But these are based on non-DRM aspects of those services.

Bottom line

Rethinking flexibility, transparency and privacy in a long term perspective would further improve the quality of the INDICARE State-of-the-Art-report.

Sources

- Anderson, Chris: The Long Tail. Forget squeezing millions from a few megahits at the top of the charts. The future of entertainment is in the millions of niche markets at the shallow end of the bitstream. Wired Magazine at http://www.wired.com/wired/archive/12.10/tail_pr.html
- Helberger et al. (2004): Helberger Natali (ed.); Dufft Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich: Digital rights management and consumer acceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report, Amsterdam, December 2004; http://www.indicare.org/soareport

About the author: *Timo Ruikka* is Vice President, Industry Initiatives at Nokia's technology Platforms unit. Contact: timo.ruikka@nokia.com

Status: first posted 07/03/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=83

Editorial of INDICARE Monitor Vol. 2, No 2, 29 April 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: In this editorial we announce a new INDICARE deliverable and introduce the articles of this issue of which most focus on DRM in the field of scientific publishing and libraries. As the use of DRM systems in this broad application field is complex and raises many questions we will continue to address it in the INDICARE Monitor.

Keywords: editorial – INDICARE

INDICARE news

INDICARE was invited by the European Commission to the workshop "Towards reaching consensus on Digital Rights Management" held in Brussels on the 6th of April, 2005. The aim was "to share the result of the informal public consultation and the outcome of the High Level Group, and where possible to further explore ways to reach consensus on DRM" (European Commission 2005). *Carsten Orwat*, co-ordinator of project INDICARE, gave a presentation titled "Analysis of consumers' issues and paths for concrete approaches" which is available online like the other presentations (European Commission 2005; Orwat 2005).

This month INDICARE made available a compilation of all INDICARE Monitor issues of the first year 2004/2005 in a single volume. In a corresponding INDICARE article we briefly present this publication adding a bit of hindsight and a bit of foresight.

About this issue

When we posted our call for papers for this issue on "science, higher education, and libraries" to an e-mail list of librarians the immediate reply was that DRM has no business in this field at all because of its character as a space of academic freedom. Open Access would be the appropriate answer (cf. INETBIB 2005). The four thematic articles we present in this special issue all recognize the special status of this field, however the authors come to a rather different conclusion about the role of DRM in there. In other words, sympathy for the rights of creators and cultural institutions like libraries makes them advocate prudently for a cautious use of DRM systems in these areas.

The use of DRM technology in this field need not necessarily be a fall from grace of mankind.

- First it seems to be often overlooked that the *expression of rights* is not per se the enforcement of rights, and that well received approaches like Creative Commons are in first place this: a transparent expression of rights. Therefore, talking about CC is also talking about DRM.
- Second, what DRM technology is and what it is not depends. For example, safeguarding integrity and authenticity of documents is safeguarding rights of creators and consumers. Technologies guaranteeing integrity and authenticity such as digital signatures or watermarks are in this sense contingent. A one man's security technology is another man's DRM technology.
- Third, in some cases DRM systems may indeed be a solution to leverage fair use exemptions. In the library context these include the right to lend, the right to preserve, the right to supply documents to third parties, the right to share.

Taking DRM as a *béte noir* – to use the expression of Richard Poynder here –- is apparently not the best approach to cope with the complexity of legal, economic and technical IPR matters. Reducing complexity may correspond to the logics of social movements facing intransigent opponents, but a balanced approach it ain't.

In this issue *Marieke Guy* and *Brian Kelly*, UKOLN, Bath, discuss the use of CC for digital libraries presenting the case of a project funded by JISC (Joint Information Systems Committee) in the UK. Their conclu-

sion is that comprehensible expression of rights is of great benefit, and that CC licences are about removing the barriers to sharing information.

Next, *Richard Poynder*, a freelance journalist and an expert in digital assets, investigates the role of digital rights management in Open Access. He starts where Marieke Guy and Brian Kelly had ended, stating that inserting machine-readable rights information into digital content like CC (in order to control how it is used) is "digital rights management". He can show that DRM, understood as a "set of tools to help creators maximise usage of their work" could support the Open Access movement especially with respect to the "green road" of OA, i.e. "self-archiving" of papers which are published by traditional commercial journal publishers.

Pasi Tyrväinen writes about fair use licensing in a library context. He claims that it is possible to support library exemptions and still maintain a high level of privacy with DRM systems. DRM systems are presented in his model as an enabler of the legal library exemptions. It is particularly interesting to see how – given an appropriate design of DRM systems – new business models may emerge from a closer interaction of public institutions and publishers. Libraries as superdistributors is just one of the ideas Pasi Tyrväinen puts forward in the three scenarios outlines.

Karen Coyle, a well known consultant in the library field, focuses her article on the role of digital rights management with respect to one particular library function, namely lending. She discusses primarily the state of the art in lending electronic books and audio books. Her conclusion is that for libraries to manage and lend published materials in digital formats some controls are required. She also concludes that digital products lead to new relationships between publishers and libraries involving DRM systems. Today however as she points out there are important issues not yet solved with respect to acquisition and lending of digital materials. To achieve a win-win situation, both, libraries and publishers, have still to learn.

Out of focus, but with high relevance for the role of DRM in the preservation of cultural heritage, *Michael Rader*, ITAS, investigates the reissue of historical recordings. The preservation of the audio heritage is largely being undertaken by small enterprises who invest a lot in audio restoration. Reissues of historical material have generally not been protected against copying although such work is protected as intellectual property and although piracy for commercial purposes is significant. This brings in DRMs as an option to stop abuse. Studying a particular case, Michael Rader concludes that watermarks might be the best solution not to restrict consumer rights on the one hand and to facilitate the detection of "pirated" works on the other hand.

Last not least, we can include again comments on the INDICARE state of the art report. This time *Manon Ress*, director information society projects at CPTech (a non-profit organisation) hints particularly to the international dimension of DRM and the concerns of developing countries in this respect.

Bottom line

In the next issue of the INDCARE Monitor we will continue the focus theme addressing further issues like "Science Commons", DRM and document supply centres, or DRM and preservation. If you feel stimulated to get involved in the debate about DRM in the field of "science, higher education, and libraries" feel free to propose a topic and to write for the INDICARE Monitor about it. The CfP with a list of topics we find relevant is still available (see INDICARE CfP 2005).

Sources

- European Commission (2005): DRM Workshop 2005 "Towards reaching consensus on Digital Rights Management". Speeches and Presentations: http://europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/events/index_en.htm#drm_workshop_2005
- INDICARE CfP (2005): http://www.indicare.org/tiki-page.php?pageName=CallForPapers

- INETBIB (2005): Re: CfP DRM in the field of science, higher education, libraries: http://www.ub.uni-dortmund.de/listen/inetbib/msg26916.html
- Orwat, Carsten (2005): Analysis of consumer issues and paths for concrete approaches. Presentation at the EC DRM Workshop 2005 available for download at http://europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/doc/drm_workshop_2005/indicare.ppt

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 29/04/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=99

QA Focus information for digital libraries

A case study of CC implementation

By: Marieke Guy and Brian Kelly, UKOLN, Bath, United Kingdom

Abstract: Creative Commons (CC) licences are a way to clarify the conditions of use of a work and avoid many of the problems current copyright laws pose. This article describes how a CC licence has been used to maximise take-up of the deliverables from QA Focus, a JISC (Joint Information Systems Committee) funded project. It then looks at CC's potential in the European academic sector and discusses relevant issues.

Keywords: case study – copyright law, cultural heritage, Creative Commons, higher education, libraries – United Kingdom

What is Creative Commons?

Creative Commons (CC) was started in 2001 by *Lawrence Lessig* as a consequence of an *un*successful law suit. Lessig had put in a complaint at the US Supreme Court to prevent fifty-year copyright (following the death of the creator) being extended to seventy-years. As this failed, CC was an attempt to "redesign copyright from within" (cf. Dreier 2004).

The eleven CC licences are written using an American legal model and are available to download from the Web site. They allow copyright holders to assign a mixture of four different conditions (attribution. non-commercial**,** no derivative works, share alike) to their works. The aim is to clarify the conditions of use of a work and avoid many of the problems current copyright laws pose when attempting to share information. Each license is expressed in three ways: legal code, a commons deed explaining what it means in lay person's terms, and a machine-readable description in the form of RDF/XML (Resource Description Framework/Extensible Mark up Language) metadata. Copyright holders can choose to embed the metadata code in their HTML pages, which will then aid retrieval.

Take up of the licences has been very popular, but because their current wording does not work well with the law in other countries the International Creative Commons Project (iCommons) was instigated to adapt them for use outside the US. At the end of March 2005 the process of writing new licences has been completed for fourteen jurisdictions. Ten jurisdictions, including the United Kingdom, are at the finalising stages.

Creative Commons and the education sector

The CC licences obviously have a lot to offer artists creating text, audio, video and images for use on the Web. But what potential do

they have for public sector communities, such as the academic and cultural heritage sectors? Within higher and further education many publicly funded bodies are involved in creation of resources that will aid learning and teaching of students and enhance research opportunities. One way to encourage use of these materials is by assigning CC licences.

A Creative Commons case study: QA Focus

QA Focus was funded by the JISC (Joint Information Systems Committee) in the UK to develop a quality assurance (QA) framework which would help ensure that project deliverables funded under JISC's digital library programmes were functional, widely accessible and interoperable. The project, which was provided by UKOLN (a national centre of expertise in digital information management based at the University of Bath) and the AHDS (Arts and Humanities Data Service), successfully developed a quality assurance (QA) framework and a wide range of support materials.

Towards the end of the project the decision was taken to make QA Focus briefing papers available under a Creative Commons licence as part of the project's exit strategy. The project deliverables are to be available for at least three years after the end of funding, as required by the funders. However the project team were concerned that a passive approach would not be effective in maximising the project's impact across the community and that the approach advocated and lessons learnt could be forgotten or ignored. There was also a concern that the project's deliverables would become invalid or inaccurate over time, as a result of technological, legal, etc. changes. To ensure the deliverables continued to promote good practice in the long-term, a policy was developed to allow free use and modification of briefing papers.

What licence?

After discussions it was decided that users should be allowed to adapt and refine the QA Focus resources, enabling them to reflect local requirements, and to be distributed without seeking permission. A number of possible licence models were investigated and three approaches considered:

1. Develop a bespoke licence
2. Modify an existing licence
3. Use an existing licence.

As the QA Focus framework encourages use of interoperable open standards an existing licence that matched requirements was considered the most effective route. There are several licences that encourage users to improve, manipulate, or build on existing work in any way (General Public Licence, Mozilla Public Licence, etc.). These place importance upon collective efforts to improve a digital resource rather than the more restrictive requirements of classical copyright. However many are primarily intended for software code and cannot be applied to information papers without modification.

After a review of available options the Creative Commons licence was chosen mainly because it is easy to understand by non-experts and widely recognised within the academic community.

CC version 2.0 offers six licences that allow unrestricted distribution but tailor specific use of the resource e.g. non-commercial, no-derivatives, etc. To satisfy the QA Focus requirements a CC licence was chosen that:

- Allows others to copy, distribute and modify briefing papers, on the provision that credit is given for the creation of the original documents (attribution)
- Is used for non-commercial purposes only (non-commercial)
- Specifies that derivatives must be classified under the same licence (sharealike).

Confirmation was obtained from host institutions to ensure they supported the policy decision and the recommended licence.

The choice of an existing solution significantly reduced the time required to develop and implement a licence. It was agreed that the licence would only apply to the briefing documents as the case studies contained project-specific information which would be inappropriate for others to modify. The decision also avoided the need to spend

time in obtaining permission from third parties to apply this licence to their materials.

The briefing papers were updated to include the CC logo and text. In addition the machine-readable description of the licence was embedded in RDF format on the HTML pages.

Discussion

The assignment of CC licences to the QA Focus briefing papers was a relatively straightforward process, but there are a number of issues that need to be considered before committing to a CC licence.

Legal status of CC

One area for concern in the past has been that the legal status of CC licences in the UK has yet to be clarified, although consensus is very near indeed. The same applies to many other European countries. However if the licences have no legal standing this should make little difference to those wanting to share resources. Until the time each country's licences become legal they will at least provide an indication of intention. QA Focus felt that this slight uncertainty should not hinder the policy decisions or the implementation of the licences.

Free availability and/or income generation

Another area for consideration is the tension between allowing resources to be freely available and the need for income generation. Although use of a CC licence is principally about allowing resources to be used by all this does not mean that there has to be no commercial use. One option is dual licensing, which is fairly common in the open source world. A copyright holder can chose to have a business model, which involves licensing their work for free alongside a commercial licence. MySQL, TrollTech, Red Hat and Sleepy Cat are all software developers who have all successfully used a dual licensing approach. The commercial work can have some form of added value, such as extra editorial content. Distributing work under a CC licence is also a very good way of advertising your expertise, potential as a speaker etc. Many feel that their academic writing makes them more money through advice giving than it ever would through article sales.

CC not always appropriate

When choosing a CC licence or working on a policy for the use of such licences it is vital to take into account scope. The same CC licence may not be appropriate for all resources available and sometimes a CC licence may not be appropriate at all, for example when external people have also contributed to work; as was the case with the QA Focus case studies. When using work commissioned from external parties it is also important to clarify the rights issues prior to publishing.

Expected impact of using CC licenses

As mentioned earlier, using a Creative Commons licence, as a means of maximising impact across the community, was part of QA Focus's exit strategy. At present there is no formal proof that use of the licences has increased impact, although interest in QA Focus documents by both the community and funding bodies continues. At present an official announcement of the documents' CC licence status has yet to be made, mainly because the QA Focus team are waiting for CC to have legal status in the UK. Once wider dissemination takes place QA Focus will be monitoring closely use and modification of the documents through site statistics and close watch of the community. Using works that have CC licences attached will be easier in the future as more search engines allow searching of the machine-readable code embedded in pages. Search engines like Google and Yahoo now allow users to search for freely available material, but at present do not index UK CC space. In the future this could provide richer searching without any additional effort needed within institutions and if felt to be useful could provide motivation for dedicated searching tools within the community. Adding a CC license could have significant impact on shaping Internet user's behaviour as they may well search initially for resources which have liberal licence conditions.

What can Creative Commons offer the European academic sector?

The use of CC licences for academic resources is an area of great potential. Many academic organisations have a vast amount

of material available for users. Making it clear to these users, through a comprehensible expression of rights, how these resources can be used is of great benefit. It will allow resources to have a consistently wide impact and will help minimise difficulties in repurposing in the future. In the UK JISC is increasingly encouraging reuse of learning resources and CC licences are a way to achieve this goal.

Recently many academic organisations have begun to use CC licences as part of their preservation strategy. Projects like the UK Web Archiving Consortium Pilot Project are investigating the long-term feasibility of archiving selected Web sites. Rights issues cause many problems and having them resolved prior to the end of a project can really help uptake of resources.

In awareness of the potential of their licences for the academic sector Creative Commons have begun initiating a number of academic focused activities. Most notably in January 2005 they launched Science Commons, an exploratory project to apply the philosophy of Creative Commons in the realm of science. The mission of Science Commons is to encourage scientific innovation by making it easier for people to share scientific intellectual property.

Bottom line

CC licences are about removing the barriers to sharing information. Surely this is what education is all about.

Sources

- AHDS: http://ahds.ac.uk/
- Creative Commons: http://creativecommons.org/
- Creative Commons Search: http://search.creativecommons.org/
- Dreier, Thomas: Some rights reserved. INDICARE Interview by Bettina-Johanna Krings. INDICARE Monitor Vol. 1, No 4; http://www.indicare.org/tiki-read_article.php?articleId=40
- Open Source Software Advisory Service: http://www.oss-watch.ac.uk/
- QA Focus: http://www.ukoln.ac.uk/qa-focus/
- UK Web Archiving Consortium: http://www.webarchive.org.uk/
- UKOLN: http://www.ukoln.ac.uk/

About the author: *Marieke Guy* works for UKOLN, a centre of expertise in digital information management based at the University of Bath. She is currently a member of the Interoperability Focus team, publicising and mobilising the benefits and practice of effective interoperability across the library, information, education and cultural heritage communities. Interoperability Focus is a national activity, jointly funded by the Joint Information Systems Committee (JISC) of the Further and Higher Education Funding Councils and Museums, Libraries and Archives Council (MLA). She previously worked on the QA Focus project. Contact: by phone 01225 385105, e-mail: M.Guy@ukoln.ac.uk.

Brian Kelly also works for UKOLN and is UK Web Focus, responsible for providing advice on Web technologies to the UK higher and further education and cultural heritage communities. He was the project manager for the QA Focus project, which developed a quality assurance framework for digital library development work. Contact. by phone 01225 383943; e-mail: B.Kelly@ukoln.ac.uk

Status: first posted 05/04/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=92

The role of digital rights management in open access

By: Richard Poynder, Freelance Journalist, United Kingdom

Abstract: Growing conviction that scientific progress will significantly benefit if scholarly articles and research papers are made freely available on the Web has given rise to the Open Access (OA) movement. While there is some awareness that OA articles may require digital rights management (DRM), there is currently only low-level interest in the topic, with many OA advocates maintaining that it has no relevance to OA. The issue is complicated by the fact that there are currently two ways in which research papers are made OA, each of which has different implications from a rights point of view.

Keywords: policy analysis – copyright law, Creative Commons, DRMS design, open access, scientific publishing, stakeholders

Introduction

OA has gained a lot of traction over the last year, but it has also attracted considerable resistance from commercial and society publishers. Since they currently generate substantial incomes from selling subscriptions to their journals scholarly publishers fear that if research is made freely available on the Internet these revenues will be significantly threatened.

Given the consequent struggle simply to make Open Access happen many OA advocates argue that worrying about DRM today could prove a distraction from the more important task of "freeing the refereed literature."

Since many also view DRM as synonymous with the use of "technical measures" designed to restrict access, rather than as a broad set of tools for managing rights in a digital environment, there is a tendency to see DRM as an issue for proprietary interests alone. The danger is, however, that if the OA movement fails to engage with the topic those proprietary interests may set the DRM agenda, to the possible detriment of OA.

Nevertheless, some preliminary work on DRM is being done by the OA movement, and the growing success of the Creative Commons (cf. sources) may encourage OA advocates to take a greater interest in the topic.

What is DRM?

Any discussion of DRM in the context of OA has first to seek to define the term. The continuing controversy surrounding P2P and illegal file swapping, for instance, has led many to conclude that DRM amounts to little more than "locking up" content with electronic padlocks. Indeed, since this perceived emphasis on restricting access is viewed as the very antithesis of OA, DRM has become the *béte noir* of many OA advocates.

What this overly narrow view of DRM overlooks, however, is that digital rights management implies something broader than access control alone. It can also be used, for instance, to ensure correct author attribution, to certify document integrity and provenance, to prevent plagiarism, and indeed to enable creators assert their rights in ways that encourage – rather than restrict – access.

It may be helpful in this regard to view DRM as a two-layered cake. In this model the first layer consists of metadata that define the usage rules (rights) associated with the content. Then on top of this can be placed an (optional) second layer of software-imposed limitations on copying, printing, viewing etc. (i.e. technical measures) in order to enforce the usage rules.

Some OA advocates argue that neither layer is relevant in an OA environment. After all, they say, the aim of OA is to make research papers available to everyone, without restriction. It may be that the use of technical measures – even for apparently harmless purposes such as ensuring document integrity – will prove "politically" unpalatable for the OA movement (although Frederick Friend's INDICARE article (Friend 2004) appears to

demur on this). There are, however, strong reasons for arguing that the use of rights metadata does have an important role to play, and will for this reason be the main focus of this article.

What authors require

It is clear, for instance, that in making their research freely available on the Web researchers have no intention of giving away their IPR. Their only aim is to allow others to read and build on their work without facing the obstacle of the toll-barriers represented by increasingly expensive journal subscriptions.

In fact we know researchers want to maintain control over their work on the Web because they have told us so. In 2002, for instance, when the JISC-funded Rights MEtadata for Open archiving (RoMEO) Project (cf. sources) asked researchers for their views 55 percent of those surveyed (both OA and non-OA authors) said they wanted to limit usage of their works to certain purposes – e.g. educational or non-commercial.

And while over 60% were happy for third parties to display, print, save, excerpt from and give away their papers, they wanted this to be on condition that they were attributed as the authors and that all copies distributed were done so verbatim.

What RoMEO made clear, says *Steve Probets*, a lecturer in information science at UK-based Loughborough University who was involved in the RoMEO Project, is that "authors *are* interested in maintaining some form of control over who can do what with their articles."

As *Brian Simboli*, a science librarian at Lehigh University in Bethlehem, PA puts it: "The shift from toll-access to open access may (illogically) encourage people to assume that the whole concept "intellectual property" has or should undergo some sort of sea change. Intellectual property is still intellectual property, regardless of how it is accessed."

Some rights reserved

What the RoMEO survey also revealed, however, is that the "all rights reserved" model of classical copyright is more than most researchers want. "[T]he protection offered [to] research papers by copyright law," the report concluded "is way in excess of that required by most academics."

In other words, when releasing their work on to the open seas of the Web OA authors are interested in asserting only some of the rights of traditional copyright (e.g. the right to be named as author), while waiving other rights (e.g. the right to copy or make derivative works). That is, their wish is to make their papers available on a "some rights reserved" basis.

But if researchers don't make clear to their readers on what basis a paper has been released, how will their readers know? They may mistakenly assume, for instance, that a paper has been made available without any restriction on its use and reuse, as if it had simply been placed in the public domain. Alternatively, they may feel constrained about using a paper in the more liberal way the author intends, for fear of legal reprisal

Consequently, if they dismiss DRM OA authors risk depriving themselves of a useful mechanism for specifying on what basis they are making their work "freely" available.

Expression of rights

For this reason, in 2002 Project RoMEO began developing an XML-based system designed to express rights and permissions in an OA environment. These issues are not unique to OA authors however. Motivated by the same desire to provide greater licensing flexibility for web-based content, for instance, in 2002 a number of intellectual property lawyers, including *Lawrence Lessig* (cf. sources) and *James Boyle* (cf. sources), founded Creative Commons (CC).

By separating out the basket of rights provided by classical copyright Creative Commons aims to give creators greater flexibility to mix and match those rights they wish to assert, and those they want to waive.

The applicability of Creative Commons to OA was immediately apparent to the Project RoMEO team, who incorporated CC licences into the work they were doing. Explains Probets: "[T]he feelings of the Romeo Project were that the Creative Commons li-

cences would be sufficient to specify the majority of restrictions/conditions required by authors (e.g. that authors are attributed, or that derivative works or commercial uses are allowed)."

Probets, however, questions whether inserting rights metadata into OA papers can be classified as DRM. "I'm not sure that I would regard these licences as a DRM solution", he says. "[They] indicate the ways the work can be used; they do not technically enforce that these conditions/restrictions are applied."

This, however, is surely too narrow a view of DRM. How better to describe the process of inserting machine-readable rights information into digital content in order to control how it is used than "digital rights management"?

Others argue that utilising rights metadata without any means of enforcing their prohibitions is pointless. By the same reasoning, however, we might conclude that it is a waste of time creating any rule, or law, unless it can be physically enforced at the point of potential infringement. We also know that anyone happy to infringe copyright law can circumvent most if not all the electronic padlocks devised to date.

Two roads to OA: The case of the "Gold Road"

For researchers wanting to better manage the rights in their papers, however, there is a more immediate problem than enforcement – namely how they establish and define their rights in the first place. And since there are two ways in which researchers can make their papers OA a one-size-fits-all approach is not currently possible.

For researchers using the "Gold Road" to OA matters are relatively straightforward: they can simply publish in one of the new-style scholarly journals produced by OA publishers like BioMed Central (BMC) (cf. sources) and the Public Library of Science (PLoS) (cf. sources). By reversing the traditional subscription model and charging authors (or more likely their funders) a fee to publish, rather than charging readers to read, golden publishers are able to make research papers freely available on the Web without any access costs.

More importantly, by treating publishing as a service provided to the author, rather than as a property transaction in which the publisher acquires copyright in return for publishing a paper, both BMC and the PLoS are happy to use the Creative Commons Attribution Licence (cf. sources) as a default option. The terms of this licence are printed as a copyright notice on all their articles, as well as being inserted into them as machine-readable metadata.

Why that particular licence? Because, explains PLoS' *Andy Gass*, the CC Attribution Licence best meets the OA criteria outlined in the Bethesda (cf. sources) and Berlin OA declarations (cf. sources). These, he says, specify that in making their papers OA authors grant "to all users a free, irrevocable, worldwide, right of access to, and a license to copy, use, distribute, transmit and display the work publicly, and to make and distribute derivative works, in any digital medium for any responsible purpose, subject to proper attribution of authorship … [as well as] … the right to make small numbers of printed copies for their personal use."

But while the Gold Road is the most logical route for researchers wanting to make their papers OA there are today only 1,600 (out of a total of 24,000) golden scholarly journals in which to publish.

Two roads to OA: The case of the "Green Road"

For this reason many researchers opt instead for the "Green Road". Rather than publishing with an OA publisher, they continue to publish in traditional subscription-based scholarly journals, but then "self-archive" an electronic copy of their papers, either on their home pages, or in an e-print archive such as their institutional repository or a centrally-based archive like PubMed Central (cf. sources) or arXiv (cf. sources).

However, the rights situation on the green road is complex, since traditional subscription-based journals generally insist that authors assign copyright as a condition of publication. As a consequence, researchers relin-

quish all control in how their IPR is managed. The RoMEO study, for instance, found that in 90 % of cases authors are asked to transfer the copyright in their papers. Moreover, while 92 % of scholarly journals now allow their authors to self-archive it is a far from ideal solution. As authors are not permitted to use the publisher's PDF, for instance, the self-archived version may be somewhat different from the publisher's version.

More problematically, the rights status of self-archived papers is vague and frequently misunderstood. Indeed, there are reasons to believe that general confusion and uncertainty over copyright represents one of the greatest obstacles to self-archiving today, and perhaps explains why still only 15 % of authors self-archive. "The fact is that copyright raises its head all the time when authors are asked about OA, and it is acting as a deterrent to self-archiving," says *Alma Swan* (Swan 2005), co-founder and director of UK-based scholarly publishing consultancy Key Perspectives (KPL). "So it can't be ignored".

The solution, suggests *John Ober*, director of the policy, planning and outreach office of scholarly communication at the California Digital Library (cf sources), is for publishers to "turn their publication copyright policies into the appropriate 'set' of Creative Commons elements"

This would clarify the situation over self-archiving, confirm its legitimacy, and so give self-archiving authors the same transparency over rights as is currently available to those publishing in golden journals. As a consequence OA would receive a significant boost.

Reducing the value of self-archiving

Far from helping to facilitate self-archiving, however, most subscription-based publishers today appear more intent on emasculating it. The fact is that as research funders like the National Institutes of Health (NIH) (cf. sources) and Wellcome Trust (cf. sources) increasingly encourage researchers they fund to self-archive their papers, publishers are becoming more and more concerned that their revenues are under serious threat. In response, they are actively seeking ways in which they can hobble self-archiving.

Having succeeded in persuading the NIH to water down its policy on public access to research (cf. NIH 2005), for instance, more and more publishers are insisting that papers are only self-archived on an embargoed basis, demanding delays of between 6 and twelve months between publication and self-archiving. This, say critics, significantly reduces the value of self-archiving, particularly in areas like biomedicine.

Publishers are also insisting that authors provide a link from the archived version to the official version of the article on the publisher's web site, and that they include the article's unique Digital Object Identifier (DOI) (cf. sources). The aim is to drive users away from the free version of the article that has been self-archived, to the for-fee version on the publisher's web site.

The next stage in this strategy may be for publishers to change direction and, instead of prohibiting authors to self-archive the publisher's PDF, to actively encourage it. This would give publishers an opportunity to reassert their ownership of the article, to reinforce their brand, and to charge authors in the process. But the real attraction is perhaps that the PDF file format is ideally suited to the use of second-layer DRM (technical measures) enabling publisher-determined usage rights to be incorporated into the articles.

The logic here is compelling. After all, as *Chris Barlas*, a senior consultant at Rightscom (cf. sources) points out, to date scholarly publishers have seen little need for DRM. As he puts it: "[M]ost of the STM publishers currently use some kind of subscription system with password protected access to sites as their form of protection." As scholarly papers increasingly leak out of these proprietary databases, however, publishers will surely want to establish new ways to protect their proprietary interests.

Certainly Springer Science+Business Media (cf. sources), the second largest STM publisher, has begun to go down this road. While it permits authors to self-archive their own versions of papers, Springer now also invites them to self-archive the final published PDF. To do this, explains Springer's executive vice president corporate communications

Sabine Schaub, authors can purchase Springer's PDF file from DRM vendor Aries, to whom Springer has outsourced the function. Aries will then "download the article from Springer Link [Springer's online database], wrap it with a DRM system called DocuRights, and send it to the author for posting or distribution".

Once it is encased in DocuRights, explains Aries' *Lyndon Holmes*, the article becomes a "pay-per-view object" with usage rules determined by the publisher. "The publisher can, for instance, specify the number of computers a particular PDF can be opened on". Amongst other things, DocuRights also allows publishers to restrict the number of times a paper is printed and/or viewed.

The attraction to researchers is that using the publisher's PDF allows them to offer the final, definitive version of their article, in a clean professional format. Moreover, since today 78 % of authors who have never self-archived are unaware of how to go about it publishers are clearly in a powerful position to persuade them that archiving a PDF reprint is a better way of providing OA. However, while authors will still be able to provide Open Access (by themselves prepaying for usage) it is not the kind of solution envisaged by OA advocates.

Take the initiative

Confronted by continuous publisher foot dragging over OA some have concluded that, rather than accepting whatever terms publishers impose, it is time for authors to take the initiative over rights. To this end the Scholarly Publishing and Academic Resources Coalition (SPARC) (cf. sources) has produced a downloadable Author's Addendum (SPARC 2005) that researchers can print and attach to the publication agreement publishers ask them to sign on the acceptance of their articles.

The aim of the Addendum is to modify the publisher's agreement to make explicit the fact that the author is retaining sufficient rights to self-archive, and to also require that the publisher provides a free PDF version of the article – moreover, with no DRM functionality incorporated into it. More specifically, explains *Michael Carroll* a law professor at Villanova University who authored the Addendum, it ensures "that the author retains all rights necessary to grant a Creative Commons Non-Commercial-Attribution License". A second version of the Addendum that will allow the author to simultaneously reserve these rights and then grant the Creative Commons license is now in draft, explained Carroll in a recent post to the liblicence mailing list (Carroll 2005).

Will this prove acceptable to publishers? While agreeing that "the intent of the Addendum is entirely reasonable", *Peter Banks*, a publisher at the American Diabetes Association (ADA) responded to Carroll's post by cautioning that several clauses in the Addendum were unacceptable. "Were we presented with this Addendum, we would decline to publish the paper. I am quite sure a majority of publishers would do the same" (Banks 2005)

In reality it is highly unlikely that subscription-based scholarly publishers will allow authors to manage their own rights. Indeed, many have come to see copyright ownership as key to their survival. While they could adapt by converting to an OA publishing model, most publishers view this as far too risky financially, and certainly less profitable. Publishers' efforts, therefore, appear to be focused on reducing the impact of self-archiving. Embargoes are one way to do that. A more powerful long-term strategy would be to encourage authors to self-archive the publishers' version and arm it with second-layer DRM. As such, the self-archived article would potentially become a Trojan horse capable of transforming OA articles into "pay-per-view objects". Such doomsday scenarios are no doubt overblown. But they serve to remind us that ignoring rights issues could prove a risky strategy for the OA movement.

For the moment, however, most OA advocates appear happy to sit on their hands. It is, for instance, nearly two years since the funding for Project RoMEO ended. While its work was inherited by the Open Archives Initiative (OAI) rights group (cf. OAI 2004), to date most of that group's efforts have been devoted to developing rights expressions for

OA *records*, not for the underling *resources*! This means that even where OA publishers and self-archiving authors include rights metadata in their papers there is currently no OA infrastructure able to exploit those metadata to good effect.

Given the continuing scepticism over rights this is perhaps unsurprising. "It is harmless to make rights explicit in metadata, but that's not the priority", says leading OA activist *Stevan Harnad*. "The priority is the *content* (for which these metadata would be part of the decoration)". In other words, until the number of self-archived papers increases there is no point in fussing over rights. But as Swan points out, uncertainties over rights are a major deterrent to self-archiving today – suggesting the movement may face a chicken and egg stalemate.

Moreover, since the 1,600 gold journals can at most make just 5 % of scholarly research OA such a stalemate would represent a significant obstacle to the wider movement. Harnad insists, however, that all that is necessary today is for governments and other research funders to *mandate* self-archiving. After that, he says, all the other dominoes will "fall naturally (and anarchically) of their own accord".

But is that enough? After all, the NIH's decision not to mandate (but merely encourage) its researchers to self-archive appears to have been partly influenced by uncertainties over copyright. This suggests that until the copyright situation is clarified uncertainty over rights – and how they are managed – will remain a serious obstacle to OA. What better reason for OA advocates to seize the DRM nettle?

Summary and outlook

One can view DRM in two ways: as a proprietary and totalising means of locking up content and forcing restrictive usage rules on users in order to maximise revenues; or as a set of tools to help creators maximise usage of their work (without ceding ownership) by specifying what rights they wish to retain and what rights they are happy to waive.

While some question whether the use of Creative Commons licences can be classified as "digital rights management" their heavy reliance on machine-readable metadata to control usage suggests it is entirely reasonable to use the term DRM. After all, why should proprietary interests bent only on locking down content have a monopoly on the term. Why should not this overly proprietary definition be challenged?

More importantly, perhaps, the OA movement faces the clear danger that if it does not more actively promote an alternative view of DRM, then proprietary interests may succeed in foisting a more restrictive model on scholarly publishing, with the risk that some of the OA movement's recent gains could be lost. With luck, the growing success of the Creative Commons – and the recent founding of the Science Commons – may help OA advocates see the relevance of DRM, and encourage them to promote a broader definition of rights management.

At the very least, by assisting researchers to utilise more liberal Creative Commons licences when publishing in traditional journals, OA advocates could introduce greater certainty about the legitimacy of self-archiving. Not only would this provide a boost to the movement, but it would help to demonstrate that digital rights management is not just about "monetising" content, but is part of a larger initiative focused on creating a rights management regime more suited to a networked environment.

"Personally, I think DRM is really important in the context of OA", says *Herbert Van de Sompel*, a member of the OAI rights group. "It can, indeed, be about protecting authenticity of works, and avoiding plagiarism … [and] … and even CC licences would cover this. But there is another increasingly important aspect. Readers of the future will more and more be robots that will try and make sense of what they 'read' (by mining content), and present their analysis to humans. It is important that such use be explicitly allowed; in the current environment, one really doesn't know whether it *is* OK to mine content from OA repositories".

Bottom line

Until there is much greater clarity over rights, and how they are managed, the OA

movement may struggle to make significant progress. Increasingly it appears that only by grappling with these complex issues can the movement hope to achieve its objectives.

Sources

- arXiv: http://arxiv.org (ArXiv is an e-print repository covering the fields of physics, mathematics, non-linear science, computer science, and quantitative biology)
- Banks, Peter (2005): Re: creative commons licencing; http://www.library.yale.edu/~llicense/ListArchives/0504/msg00059.html
- Berlin Declaration: http://www.zim.mpg.de/openaccess-berlin/berlindeclaration.html
- Bethesda Declaration: http://www.earlham.edu/~peters/fos/bethesda.htm
- BioMed Central (BMC): http://www.biomedcentral.com
- Boyle, James: http://www.law.duke.edu/boylesite
- California Digital Library: http://www.cdlib.org/
- Carroll, Michael (2005): Re: creative commons licencing; http://www.library.yale.edu/~llicense/ListArchives/0503/msg01777.html
- Creative Commons: http://creativecommons.org
- Creative Commons Attribution Licence: http://creativecommons.org/licenses/by/2.0/
- Digital Object Identifier (DOI): http://www.doi.org/
- Friend, Frederick (2004): Who protects the un-protected? Open access publication needs DRM! INDICARE Monitor Vol. 1, No 5; http://www.indicare.org/tiki-read_article.php?articleId=49
- Joint Information Systems Committee (JISC): http://www.jisc.ac.uk/
- Lehigh University, Bethlehem, PA.: http://www3.lehigh.edu/
- Lessig, Lawrence: http://www.lessig.org/blog/
- National Institutes of Health (NIH): http://www.nih.gov
- NIH (2005): Policy on Enhancing Public Access to Archived Publications Resulting from NIH-Funded Research; http://grants.nih.gov/grants/guide/notice-files/NOT-OD-05-022.html
- Open Archives Initiative (OAI) (2004): Implementation Guidelines for the Open Archives Initiative Protocol for Metadata Harvesting. Conveying rights expressions about metadata in the OAI-PMH framework; http://www.openarchives.org/OAI/2.0/guidelines-rights.htm
- Poynder, Richard (1999): Hidden Value: How Intellectual Property Know-how Can Make or Break Your Business: Derwent Information Ltd
- Poynder, Richard (ed.) (2000): Caught in a Web, Intellectual Property in Cyberspace: Derwent Information
- Project RoMEO: http://www.lboro.ac.uk/departments/ls/disresearch/romeo/index.html
- Project RoMEO (Deliverables): http://www.lboro.ac.uk/departments/ls/disresearch/romeo/Romeo%20Deliverables.htm
- Public Library of Science: http://www.plos.org
- PubMed Central: http://www.pubmedcentral.nih.gov/index.html PubMed Central (PMC) is the U.S. National Institutes of Health (NIH) free digital archive of biomedical and life sciences journal literature.
- Rightscom: http://www.rightscom.com/
- Scholarly Publishing and Academic Resources Coalition (SPARC): http://www.arl.org/sparc/
- Science Commons: http://science.creativecommons.org
- Simboli, Brian (2005): creative commons licencing; http://www.library.yale.edu/~llicense/ListArchives/0503/msg01716.html
- SPARC (2005): Author's Addendum: http://www.arl.org/sparc/author/addendum.html
- Springer Science+Business Media: http://www.springer-sbm.com/
- Swan, Alma (2005): Open and Shut? An interview by Richard Poynder available at http://poynder.blogspot.com/2005/04/roller-coaster-ride.html
- The Wellcome Trust: http://www.wellcome.ac.uk

About the author: *Richard Poynder* is a freelance journalist who writes about information technology, telecommunications, and intellectual property. He contributes to a wide range of specialist, national and international publications, and is editor and co-author of two books: *Hidden Value* and *Caught in a Web, Intellectual Property in Cyberspace* (cf. sources).

Status: first posted 22/04/05; licensed under Creative Commons
URL: http://www.indicare.org/tiki-read_article.php?articleId=93

Fair use licensing in library context

A privacy-preserving lending service with a revenue sharing business model

By: Pasi Tyrväinen, University of Jyväskylä, Finland

Abstract: Any technical solution intended to support library exemptions and other fair use provisions has to take into account national regulation, the local use context, and the requirements of business models. In this article a model is proposed for dealing with these challenges. It is exemplified for the library context claiming that it is possible to support library exemptions and still maintain a high level of privacy with DRM systems. Finally new business models for libraries are sketched based on revenue sharing using superdistribution and delivery chain tracking.

Keywords: technical analysis – business models, copyright law, DRMS design, fair use, libraries, P2P, privacy, public sector, superdistribution

Introduction

Consumers see digital rights management (DRM) systems primarily as a tool for piracy protection in digital content distribution. These DRM systems provide access to encrypted content only on the hardware identified in a digital license. This kind of *hardware locking* restricts fair use, e.g., when lending digital material from libraries or by preventing copying content for private use. There is common agreement on the need to design DRM systems and electronic commerce business models which allow fair use (ACM 2003). Various means have been proposed to implement fair use, e.g. by implementing it with licensing rules in DRM systems (Mulligan and Burstein 2002), by licensing protocols, by watermarking, by authorising protocols etc (see reviews of alternative designs in Bechtold 2004, and Tyrväinen 2005). However, the intelligence about contextual factors needed for interpreting the legal limits of fair use cannot be 100 % implemented in the licensing rules of DRM systems, especially in the US legal context (von Lohmann 2002).

Fair use, identification and privacy

In this paper we use the term *fair use* (or fair dealing) as a general concept referring to the legally protected right of people to use content based on exemptions and limitations of national copyright laws (EU2001/29/EC, US 2000). These variations in national legislation increase the complexity of implementing it within DRM systems. Nevertheless, approximating fair use by licensing would be a useful service for the customers. With such a service one could avoid the need for costly human evaluation of fairness of use in a vast number of cases and thus encourage content providers to support fair use cases – although a small percentage of the cases would still need human intervention. In both cases identification of the use context and of the persons or the organization in question is needed.

Identification is a double-sided problem with respect to fair use. Customers registering for a media provider's service with their account identity or credit card identity can be traced and media distributors can link together all customer purchases, which threatens customer *privacy*. DRM systems connecting the right to use content products to a hardware identity enable the use of this hardware identity for tracing even when customers purchase their products from multiple vendors. However, media vendors would certainly like to identify the context in which they enable free use of products based on fair use exemptions. For example, they would like to identify the party claiming to be a library and requesting rights to lend copies to their customers. In case the library can be identified, the media provider may trust the library and let it identify the library customers, to the extent needed. Clearly, some fair use cases have higher requirements for identification of *trusted second parties* (such as the library) than what is expected from an individual

(here the third party) borrowing content from the library.

From product copy management to license management

Prior to digitization, illegal content use could most easily be recognized at the point of creation of copies. This is mostly true also for digital products. But when DRM systems are used, the focus shifts from creating copies of protected content products to the creation of licenses enabling use of the content products. In superdistribution (Mori and Kawahara 1990) protected content is distributed freely, but requires purchasing a license for use. Thus creating the licenses enabling use of the content is the context where fair use should be evaluated.

The next question is, should the usage rights declared in the licenses be based on the *identity of the person* or on the *identity of the hardware*? Use of hardware identity is commonly considered less user-friendly. However, in the library customer case, linking all the content borrowed by a customer with the customer identity would be more likely to infringe privacy than linking the products with multiple hardware identities unknown to the library.

Proposed approach for fair use licensing

Supporting privacy with product copy managers

To improve privacy we propose an arrangement, where the customer is able to get a temporal digital license from another trusted party in order to use the content on his hardware. For this purpose, the customer needs to pass some information received from the trusted library to the other trusted party. The primary role of the new trusted party is thus to create digital licenses for the customer hardware. Secondly, the trusted party should keep record of the number of product copies lent by the library with the license of the library, to satisfy the requirements of media vendors. For this reason, we refer to this trusted party as a *product copy manager* (PCM). Although this particular PCM knows the hardware identities associated with the product, it will not be able to connect the data with any identification of the customers or to connect it with other data located at the various places of purchases (or other PCMs when multiple equipment is used).

By separating multiple places of purchases, multiple trusted PCMs and multiple hardware identities we avoid many problems encountered by related approaches. These include the single dongle problem (e.g. single hardware identity) and the problem of cumulating customer data by a trusted party as observed by Knopf (2005). Note that in the approach of Knopf there exists a role of a TTP (trusted third party), while we separate the roles of a trusted second party (a library) and the role of a trusted PCM. Knopf also uses watermarks for personalizing the content for consumers while we prefer carrying hardware identification information in licenses embedded in the content or transmitting separately from the content according to the superdistribution mode. Note also, that a PCM should not be mixed with the actual DRM systems controlling the use of content (for further details see Tyrväinen 2005).

Two-phase approach for fair use licensing

In the library case the library was the second trusted party, which was identified to the extent needed for the fair use license during the license acquisition process. The third party (a customer) communicated only with the trusted second party and the PCM binding the license to a specific hardware, in the context identified by the special library license granted to the second party. This can be generalized as a two-phase approach for fair use licensing.

- In the first phase, the second party (the library) is identified to the extent needed for trusting it; the special license is purchased (e.g. a library license), and the second party will receive a license template (e.g. a library customer template), to be delivered to third parties. Special cases may require human judgement (for further details see Tyrväinen 2005 and Erickson 2003). Note that according to the EUCD fair use should be enabled only when content has been legally purchased.
- In the second phase, the third party (a library customer) trusted by the second party receives the template and acquires

the hardware locked digital licenses for his equipment from the PCM. This second process does not include monetary transactions or negotiations and can be automated.

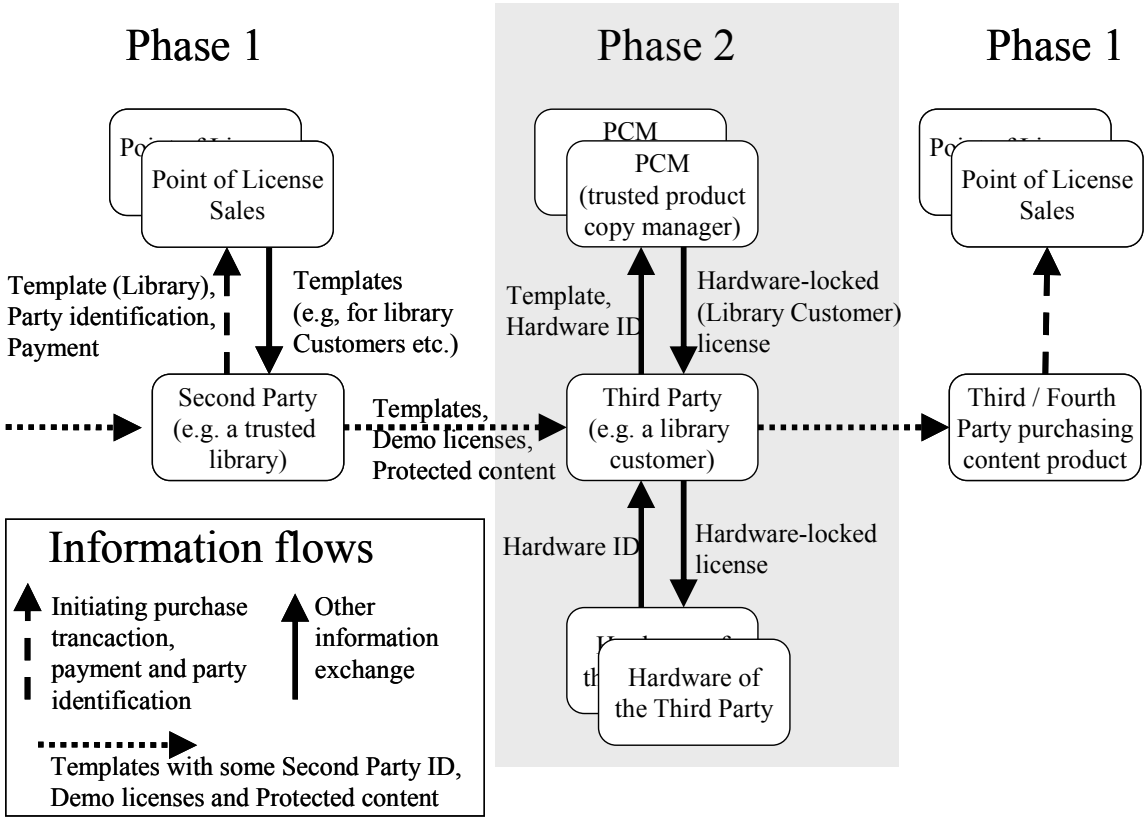


Figure 1: Two-phase model for fair use licensing

The fair use exemptions included in national law define the kinds of license templates needed; library licenses, educational licenses, and personal copy licenses being probably the most common. Each of the exemptions may require a different level of identification of the second party at the point of sales and in the templates as well as in between the second and the third party. Also the conditions of the licenses vary.

Fortunately, the same content can be used with a multiplicity of license types each defined for a specific fair use case in each national context, and the same license types can be applied to large categories of products (e.g., to all songs) simplifying the product management problems of media distributors. However, fairness will have to be determined by human judgement in some percentage of the cases even when using this approach, depending on the national regulations. The following examples will demonstrate how the context of the process is captured.

Product copy owner identity supporting privacy of personal copies

In the case of personal copies the same person purchasing a content product in the role of a second party, can acquire hardware locked licenses for other equipment with *personal copy templates* from a PCM. In this case the media distributor trusts the person to use these personal copies for personal use only, within the legal limits of fair use. The PCM can limit the number of personal copies per person for each product, for example, using *product copy owner identity* in the templates. Still the PCM is unable to identify the person behind the product copy owner identity and unable to connect the data with other products purchased by that person. However, in some cases the customer might like to be identified as the distributor of li-

cense templates using customer identity rather than the product copy owner identity known only to the point of sales selling the license to the second party.

Customer rewarding in peer-to-peer marketing

Consider a case, where a customer (the second party) has purchased a content product for private use and receives, among others things, a *promotion license* and a *distribution template*, which the customer delivers to a third party with the protected content. Using the promotion license the third party is permitted a limited use of the content on any hardware, e.g. to play the first 15 seconds of a song.

If the third party decides to purchase a personal license and uses the distribution template containing the identity of the second party, the distributor can reward the second party for the sales activity. This type of rewarding can be considered fair, but requires disclosing identity of the second party, to some extent (for further details on delivery chain tracking in peer-to-peer marketing, see Tyrväinen, Järvi and Luoma 2004).

There exists a trade-off between privacy and identification of the parties. The level of customer identification needed for customer rewarding in the peer-to-peer marketing model is not necessary for content products purchased for private use without intent to receive reward for sharing it with friends. Thus the level of tracking applied for the delivery chains needs to follow the requirements of each fair use case or business model.

New business models for libraries and other public institutions

When libraries lend content to customers, whom they have identified (face to face), the proposed approach provides a high level of privacy for the customers, whose identity is not connected with the product data in any phase of the process, and whose one hardware identity is connected with the product copy identity of the library in one PCM. However, there are also situations, where the libraries and schools would like to disclose their identity to more than one point of license sales.

In libraries and in educational use we can envision cases, where a library customer or a student at school would like to purchase the content product after getting familiar with it. In these cases the library or the school would already have been identified properly, and would certainly be very happy to receive a share of the revenue, to prop up the restricted budget of a public administration entity. The impact of schools and libraries on the purchase of content products is well known, and being able to quantify the impact would contribute to the creation of business models. This closer interaction of public institutions and media vendors can be seen either as an opportunity for the institutions or as a threat to the independence of public services.

One possible future scenario includes increased revenue from media vendors to the libraries and schools. In this scenario the libraries and schools would still purchase the content products from media vendors with prices similar to those under current discount policies. In case some of the customers or students would like to purchase the product after using it with the special license, the second party identity would be used to direct sales provision to the library or school in question. This would probably guide the purchases of libraries to follow closely their customer demand, towards the content with most marketing effort.

Another scenario includes outsourcing of content product lending to external service providers. In this scenario the technical effort and market follow-up is outsourced while the control over selection provided is kept in the hands of the library or the school, with reasonable costs.

In a third scenario the service providers would not need public funding. It would suffice to get their income solely from the media companies in the form of sales revenue sharing. This scenario is somewhat similar to the use of promotional versions or prereleases for product marketing used commonly in the software sector of content business. It is likely, that in this last scenario public libraries would be needed to maintain a balanced offering of content products for the public.

Bottom line

It is possible to support library exemptions while maintaining a high level of privacy and enabling use of personal copies with DRM systems. This includes an opportunity to gain shared revenue when lending is combined with content superdistribution and delivery chain tracking.

Sources

- ACM (2003): Special issue on fair use, Communications of the ACM, Vol. 46, No. 4
- Bechtold, S. (2004), Value-centered design of Digital Rights Management, INDICARE Monitor Vol. 1, No. 4; http://www.indicare.org/tiki-print_article.php?articleId=39
- Erickson, J.S (2003). Fair use. DRM, and Trusted Computing. Communications of the ACM, Vol. 46, No. 4, pp. 34-39
- EU2001/29/EC. Directive 2001/29/Ec of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society. Official Journal, L (167). (22/06/2001), 0010-0019
- Knopf, D. (2005): How to implement copyright exceptions in DRM systems. INDICARE Monitor Vol. 2, No. 1. http://www.indicare.org/tiki-read_article.php?articleId=87
- Mori, R. and Kawahara, M (1990): Superdistribution - the concept and the architecture. The Transactions of the IEICE, Vol. 73, No. 7
- Mulligan, D. and Burstein, A (2002): Implementing copyright limitations in rights expression languages. 2002 ACM Workshop on Digital Rights Management, Wyhdham, Washington DC, USA: ACM, 2002, pp. 15
- Tyrväinen, P. (2005): Concepts and a Design for Fair Use and Privacy in DRM. In D-Lib Magazine, Vol. 11, No. 2, http://www.dlib.org/dlib/february05/tyrvainen/02tyrvainen.html
- Tyrväinen, P., Järvi, J., and Luoma, E. (2004): Peer-to-Peer marketing for content products - Combining digital rights management and multilevel marketing, Proceedings of EC2004, http://www.jyu.fi/~pttyrvai/papers/EC2004Preprint.pdf
- US (2000): Fair use, United States Code, Section 107, Chapter 1, Title 17, http://assembler.law.cornell.edu/uscode/html/uscode17/usc_sec_17_00000107----000-.html
- von Lohmann, F. (2002): Fair use and digital rights management: Preliminary thoughts on the (irreconcilable?) Tension between them. Computers, Freedom & Privacy (April 12 2002), 9

About the author: Dr. *Pasi Tyrväinen* is Professor of Digital Media at the Department of Computer Science and Information Systems at the University of Jyväskylä. He received his doctoral decree at Helsinki University of Technology in 1994. His previous affiliations include R&D management positions at Honeywell Industrial Control and Nokia Research Center. His research interests include digital rights management, enterprise content management, communication genres, and software business. Contact: http://www.jyu.fi/~pttyrvai/ or Pasi.Tyrvainen@cc.jyu.fi

Status: first posted 24/04/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=94

The role of digital rights management in library lending

By: Karen Coyle, Digital Library Consultant, Berkeley, CA, USA

Abstract: Libraries purchase and lend a wide variety of materials, from the most common of trade items to small press publications and even ephemeral resources. They also serve heterogeneous communities with a wide range of interests, skills and resources. As cultural materials become available in new technologies libraries endeavour to make these available to their target communities. From the very earliest digital products, libraries have worked to present these to their users. Libraries are now lending electronic books and audio books using technology that is very similar to that used for the sale of these same formats. But both libraries and publishers need a paradigm shift before digital materials achieve the revolution over the Gutenberg legacy.

Keywords: policy analysis – business models, e-books, e-payment, lending, libraries, preservation – USA

Introduction

As new technologies come into being, the world's cultural objects change shape accordingly; from the clay tablet to papyrus, from the printed book to web-based documents, each takes the form of the technology of its era. Over thousands of years libraries have collected, organized, and made works available (to all, or to a select few) in these formats, and library services have developed to take advantage of the new technologies. In particular, the portability of the printed book in 18th century and beyond meant that libraries could lend works to users, and the mass production of printed texts in the 19th and 20th centuries saw a great proliferation of libraries and the extension of library use and lending to the general population.

The inexpensive reproduction of works has allowed libraries to move their energies from the conservation of objects to the dissemination of highly mobile containers. While the term "library lending" evokes an image of books for most of us, some public libraries in the United States count non-book materials such as music discs, films, and spoken books, as a full thirty percent of the materials they lend. Library lending, however, is both costly and insecure, with both wear and non-returns taking their tolls. Wouldn't it be great to be able to lend materials that could not be damaged or stolen, and that would be guaranteed to return at the appointed time? This, then, is the promise of digital lending.

Libraries and digital delivery

Libraries have been delivering works in digital formats for over a decade. The delivery of digital works to library users follows two basic models: there is the "all you can eat" model in which users have access to a database of digital materials with no restrictions on how many users can access an item at a time (although licenses may restrict total simultaneous uses to the database from any institution); the other model is an imitation of the lending of hard copy works, and is often called the "one user/one book" model. Within these two models there are different possible delivery options, with some systems presenting portions of materials on the screen but not allowing downloads or offline use, while others do allow downloading of digital items. It is in this latter case where technical enforcement of license terms comes into play, and this is the type of protection that is most often referred to as digital rights management.

The "all you can eat model" is primarily used for research materials, especially journal articles. With the development of large databases of digital full text, academic library users are well-served with instant access to a significant collection of materials. Access to these journal articles is through an institutional subscription, not unlike the subscription to the same materials in paper format. The only technical controls for these materials are on access, which is generally managed through a proxy server on the institution's network, and which limits access to

members of that institution's community. Users can download and keep copies of articles, somewhat like making a photocopy of articles in the analogue world. The downloaded articles, which are predominantly in Adobe PDF format, have no technical protection that would further restrict copying or printing, although they may be protected against alteration. This model works well for academic materials and will probably continue to do so, although there is some tension between publishers and libraries over costs and over the relationship between the digital license and the hard-copy subscription.

This model is not viable for those materials where units are normally sold individually, especially those materials that might be deemed of a "popular" nature. Books, videos, and musical recordings are in this category. These materials need to use the "one user/one book" model, and require some technical protection on the content files to satisfy publishers that the materials will not be pirated once they have been delivered to end users. In the entertainment arena we have seen the struggle between users and publishers over the unauthorized trading of works in digital form. Books and other lengthy texts have not had the same degree of problems with piracy (for both technical and market reasons), but book publishers have been cautious about delivering their products in a digital form that would open the door to piracy.

The first electronic book products were available only on proprietary hardware, such as the Gemstar (later Rocket) e-book reader. The device protected against unauthorized copying by allowing communication only with the e-book vendor site through phone lines or an Ethernet connection. Some libraries experimented with lending these e-book devices pre-loaded with a selection of books, but the devices did not catch on commercially and the e-books themselves eventually became unavailable.

The first computer-based e-book lending systems that were developed for libraries in the late 1990's, in particular the netLibrary system (cf. sources), required users to read the books online with only one page image downloaded to their computer at a time. This method was used because there was no available technical protection for downloaded files. The books were "checked out" to the library patron and could not be viewed by another library user until the lending period ended. The check out process effectively locked the book so that it could not be accessed until the current loan period ended. Although called "lending," from the user's view this was not at all like using printed books, especially in terms of the quality of the reading experience.

Library lending becomes reality

Although there hasn't been a breakthrough technology that would make electronic reading as popular as its paper counterpart, the availability of software that both facilitates the reading experience and secures the digital content has greatly increased both the willingness of publishers to make their content available and the desire of consumers to purchase that content. Digital content can now by downloaded by consumers to a variety of devices, and can be read off-line.

Libraries have been able to take advantage of the fact that the lending of digital content is compatible with the sale of that same content. In fact, OverDrive (cf. sources), the company whose software is used in book-related e-commerce, is also a major provider of electronic content systems for libraries. In a sense, library lending is the same as a sale, only with a time limit imposed. At the end of that time limit, the rights management software in the downloaded file turns off file access an thus prevents further uses of the content. The book "returns" to the library automatically with no action required on the part of the borrower.

The first lending systems had only one way for the book to return to the virtual shelf, and that was through the expiration date on the loan. This required no communication between the downloaded file and the lending system; each acted independently on the time limit. Even if a user no longer needed the item, it remained checked out and unavailable to others for the duration of the loan period, and because of this libraries were

setting very short loan periods, which was discouraging to some users. With current lending technology, users can return a book to the library at any time before the return date. Through an interaction between the checkout system and the rights technology protecting the item on the user's device. This is just one example of how developments in digital rights management (DRM) have made it possible for libraries to provide better service to their users.

Libraries purchase electronic books just like they do their print counterparts through companies that serve the library market. The information about the books is entered into the library catalogue, but instead of a number indicating where the book can be found on the shelf there is a link that takes the user to the virtual shelf of the e-book lending system. All interactions with the e-books go through the library's system, which has user information and authentication routines, and which must record the status of an item ("on shelf," "checked out") for display to library staff and users. Although the user's impression is that the e-book is in the library, in fact the books are stored on a third-party site that delivers the DRM-enabled file to the user's device. At this point in time, the economics of DRM technology do not allow libraries to securely store and deliver electronic files.

Points of purchase for e-books offer consumers a choice of formats corresponding to various brands of reading software and the particular DRM of that brand. Libraries have to select a format when they purchase an e-book. If they wish to have more than one format available they have to purchase each separately, and generally at full price. For this reason, libraries tend to limit their selection to the most widely available software, which today is the Adobe Acrobat format. The Adobe Reader software is available for free for most operating systems, including those of the common hand-held devices which are popular with e-book enthusiasts.

Lending beyond text

Because lending uses technology that is very similar to the technology for sales, in essence any digital formats that can be sold can also be loaned by libraries once the additional lending capabilities are in place. A small number of libraries are beginning to lend audio books. Books "on tape" are very popular items in libraries that lend them, especially in areas where automobile commuting is common. Library lending follows the same model of services as provided by sales points for these files: end users can download the audio book to a personal computer or to a mobile device, or they can burn the audio book onto CDs. All of these actions are secured by the lending system to prevent unauthorized copying of the files to other devices. Although the CD format is unprotected, only uncompressed files are released for these copies. This is the same format that is used in the CD audio books that are sold in stores, and therefore represents a level of risk that publishers have found acceptable.

Lending of musical works and of motion pictures could become technically possible but are not currently available. Some of the issues relate to industry expectations, and others to technology capabilities such as bandwidth. It may also be the case that rights management techniques that are sufficient to protect one form of content will not be suitable for all forms of content. As we see with the relatively low level of protection on academic journals, risks vary both by format and by commercial expectations for different materials. It does appear, though, that the level of rights management that is appropriate for the sale of content is also that which protects the content for library lending.

Libraries: what do they really want?

Lending of e-books and digital audio books by libraries is still very new, and libraries are in the learning stages in terms of what works and what doesn't. From the point of view of libraries, there are some unsolved issues relating to the acquisition and lending of digital materials. These are:

- Book publishers have a revenue model based on the hard copy world of sales of physical items, but the technology of digital lending does not allow the libraries to actually take possession of the digital item. Libraries must purchase items over which they cannot exercise normal rights of ownership.

- The storage, delivery, and control of digital materials require sophisticated secure systems. These systems are not affordable to individual libraries, but are usually run as a central service by a vendor. Libraries are dependent on the vendors both for current services and for long term access to materials they own. Should companies fail, and some have, libraries lose access to books they have purchased.
- There is no one standard format for digital delivery, yet each formatted version of an item requires a separate purchase. At the same time, libraries cannot forego obtaining materials in analogue formats, so increasingly libraries are needing to purchase multiple copies of an item to satisfy the format needs of their clientele.
- Library services attempt to provide a unified view of the cultural and intellectual sphere, with items from many different publishers and sources treated equally in terms of organization and access. There are many different sources for digital materials, often with their own proprietary technology for access. This may serve the marketing of materials, but it is not conducive to end-user research or bibliographic services.
- The proprietary formats in which digital materials are issued are not suitable for long-term preservation and access.

Most of these points evidence the difficulties of a transition period in terms of content technology, where the capabilities of the new technology and the market structures in place based on earlier technology are not compatible. The use of individual copies as the basis for the market breaks down in an environment where copies are made each time a user opens a work. One of the promises of digital rights management is that it could re-focus content delivery around rights rather than copies, which could make it possible to solve some of the problems listed above. For example, libraries could be allowed to transform materials to different end-user formats as long as the total number of items in use does not exceed the library's license. The problem of the need for persistent access over time could also be solved by allowing libraries to store a specially formatted archival copy that is not delivered to end users, while at the same time they lend protected copies in consumer formats. All of these capabilities require DRM that guarantees that the digital files will be secure and that publishers will receive payment as agreed.

What this will eventually mean is a move from a market based on copies to a market based on rights. The technology that this will require is not yet in existence, but the required changes are not just technological; huge leaps must be made in the intellectual property markets and in the habits of librarians and those they serve. Some desired features, such as the ability to lend multiple copies when user demand increases for a particular title, are well within the capabilities of the current lending technology but do not meet the accounting needs of publishers, whose system of royalty payments makes the use of micro payments particularly complex. Improvements in the e-commerce middle layer will allow us to experiment with new models of secure file delivery.

Bottom line

Many library professionals view digital rights management as a restriction on use, and it is true that the capability to create restrictive technologies exists. But for libraries to manage and lend published materials in digital formats will necessarily require some controls. If libraries can learn to view digital formats as delivery mechanisms rather than as a substitute for physical copies we may be able to develop a suitable paradigm that is beneficial to libraries and to their users. And if publishers can transition to a revenue model that is based on licenses rather than copies, we will be able to make use of the advantages that digital formats have over their analogue equivalents.

Sources

- Ebook Library (EBL): http://www.eblib.com/
- Libwise: http://www.libwise.com/
- netLibrary: http://www.netlibrary.com/

- Open eBook Forum: http://www.openebook.org/
- OverDrive: http://www.overdrive.com/

About the author: *Karen Coyle* is a librarian with almost three decades of experience in digital libraries. She writes and speaks on both technology and policy issues. More information on her work is available at http://www.kcoyle.net.

Status: first posted 24/04/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=95

Preservation versus exploitation

Dilemmas in the reissue of historical recordings

By: Michael Rader, ITAS, Karlsruhe, Germany

Abstract: While the market for the reissue of historical recordings seems sufficiently attractive for there to be multiple reissues of the same recordings, there is the additional aspect of the preservation of the audio heritage. This is largely being undertaken by private actors who invest substantial time and money in audio restoration and research. A recent court decision acknowledges that such work is protected as intellectual property. Even so, different interests in this field are a barrier to enforcement of rights so that digital watermarks might prove the most acceptable solution.

Keywords: legal analysis, economic analysis – DRM users, intellectual property, piracy, preservation, public domain, watermarking

Introduction

The reissue of historical recordings has in general been very much a niche market catering for collectors rather than the more general customer. In Europe and most other regions with the exception of the US, recordings older than 50 years enter the public domain. In view of the restricted market, it might surprise bystanders to discover that there are multiple reissues of recordings considered more readily marketable, e.g. in the classical domain the works of early 20th century tenor *Enrico Caruso*, in the jazz area recordings by such household names as *Louis Armstrong*, *Benny Goodman*, *Glenn Miller* or *Django Reinhardt*. Competition will probably increase when recordings by *Elvis Presley* and the wealth of recordings from the 50s and 60s which are still heard on the radio, gradually enter the public domain in Europe.

For more casual buyers, competition is via prices, but there is in addition the aspect of sound quality which also plays a role in the preservation of the heritage of sound recordings. This preservation work is being done almost exclusively on private initiative. Sound restoration work is protected by intellectual property rights as "minimally creative work". This has been acknowledged in a recent court decision. What follows obviously also applies to films which have been restored for reissue on DVDs.

The issue

While the average consumer might want to buy historical recordings to play as a novelty at parties, because a certain type of music is currently fashionable, like swing a couple of years back, or because curiosity has been piqued by such films as "The Aviator", there have always been collectors of vintage recordings.

There have always been concerns about the durability of early recordings which were made of breakable material in the first place so that it is surprising that so many have survived until the present. There are sometimes only single known copies of recordings. In addition, there are recordings in circulation

which were never widely issued or intended for issue, such as test pressings, private recordings, recordings made for publicity purposes, all of which are of interest to some collectors or historians. Preservation is of particular interest for so-called vernacular music, meaning music outside the well-documented elite cultures. Examples are performances of jazz and blues, tango and other ethnic music, which would largely be lost without recordings. There is also interest in performances by legendary performers in the classical realm, such as the previously mentioned Caruso.

While there are collectors who jealously guard their treasures and allow no-one else to hear them, the domain is characterised largely by willingness to share and preserve for posterity. Some actors in this field state that they do not own the records, but are simply their custodians during lifetime with the duty to hand them down to future generations.

Since the major companies have little interest in the field due to limited return on investment, this is an area where small independent companies are very active. In the past, there was a very thin line separating reissue activities from piracy and one early company actually called itself "Jolly Roger" after the pirate flag with the skull and crossbones. However, gradually many recordings considered worthy of reissue have entered the public domain, at least outside the US and are thus legal. Even so, it is strictly speaking illegal to sell certain European reissues in the US. There is reluctance to take legal action against competitors due to prevailing ethos and also due to the costs of taking lawyers. Many companies are run by producers with day jobs outside the music business and these prefer to invest any money they make out of reissues on new productions rather than in legal action.

Reissue policies vary a great deal. Some obviously only want to take the money and run. They do not care about such things as audio quality or presentation and will use virtually any source. Even in the days of long-playing records, it was common practice to simply copy individual tracks or entire albums from other LPs. Other labels have ambitious programs wishing to reissue everything irrespective of sound quality and source (original recording, LP or cassette). Still others regard themselves as preservationists and take great pride in quality and presentation, sometimes going to great lengths to track down rare items and doing, or commissioning, impressive research work to unearth information about rather obscure artists by today's standards.

Audio restoration and production of accompanying material result in substantial costs. To some extent, the values in this field have changed. Instead of on "noise suppression", there is a premium on preserving the sounds originally contained in the grooves. This means that there is still demand for "new" restoration work. Although digital equipment for audio restoration is readily available, its use requires considerable skill. The best audio engineers in these fields have reputations among collectors and their name on a product is regarded as a hallmark of quality, just as certain labels have good reputations.

Probably as much for financial reasons as for any other, reissues of historical material have generally not been protected against copying in any way, so that it is easy to infringe on any intellectual property rights which might exist in the field.

The "Bear Family" court decision – acknowledgement of IPR protection for restoration work

Readers of the INDICARE Monitor will no doubt remember the "Jib Jab" incident in the recent US presidential election (cf. Böhle 2004). In this, the current copyright owners of *Woody Guthrie*'s "This Land is Your Land" took action against the owners of the JibJab website for unauthorised use of the work in a parody on the US election. One of the ironies of the case was that the melody of the Guthrie song was itself not an original composition but the reuse of a song of undetermined origin which had been copyrighted by *A.P. Carter* of the Carter Family recording artists in the early 1930s. Many references were made in the discussion of JibJab to currently available recordings by the Carter Family, most frequently to a box set

produced by a company called JSP located in London.

Precisely this box set and second box of recordings by the Carter Family were the subject of a court ruling by the Hamburg district court (Landgericht Hamburg, 3 February 2004, cf. Byworth 2004). This was the result of action taken by the German specialist label, Bear Family, against the unauthorised use, by the London-based company, of recordings originating from a 12 CD box set "In the Shadow of Clinch Mountain", which contains the complete works by the Carter Family with audio restoration work commissioned and paid for by Bear Family. Such work is protected as intellectual property even if the recordings themselves have passed into the public domain and can theoretically be reissued by anyone. Such intellectual property rights on restoration work are indicated by the (p) sign, which can also apply to a compilation.

The court decision was taken in the absence of the defendant, the owner of JSP, who had previously been ordered to refrain from the manufacturing of the box sets containing copied recordings. The conviction was for improper business practices and the court instructed the British company to provide Bear Family with all information relating to production and sales of the box sets and to provide compensation for damages resulting from production and sales.

The decision was based on testimony by an expert witness, but the decisive factor was the inclusion in both sets of a unique recording which had been tracked down by Bear Family.

While both companies' countries are members of the European Union, the Hamburg court decision had to be registered at a British court to take effect, which again required the services of a lawyer, another cost which most producers would not be willing to take on even temporarily. Even so, the court decision, which Bear Family's lawyer, *Ulrich Poser*, describes as "path breaking for the branch" (cf. Anon 2004) has actually resulted in the payment of substantial damages and has encouraged at least two more producers to take action against another German company which is notorious for its piracy practices.

A collector, who also writes for a web-based publication on film music (Schlegel 2004), describes how this German company pirated copies of film soundtracks. Among other things, he attempted to invoke assistance by the German collecting society, GEMA, which was initially very reluctant to take any action. When it finally did, it emerged that a license for intellectual property on the soundtracks had been registered in the Czech Republic, preventing action from any lawful owners.

As readers who have come this far will have guessed, piracy of audio restoration work is far from exceptional. Bear Family has thus taken the consequence of adding a water mark to its own productions. According to Bear Family director *Hermann Knülle*, such watermarks are tamper resistant, while allowing "legal" copying, for example for use on devices such as MP3 players belonging to the owner of a copy of the recording. The watermark remains perceptible even after extreme compression, independent of recording technology for copying (microphones, radio, connecting CDs to sound cards) and presumably following further audio processing by any third party. It can be "individualised" to the extent that a copy is traceable to a particular copy of a series. Of course it is inaudible (for details you may see: http://www.ipsi.fraunhofer.de/merit/media_security/).

Actor interests

Only a small fraction of all sound recordings ever made has actually been reissued. A private initiative, "Project Gramophone", which aims at making every recording ever made publicly available via the internet, has encountered unexpected problems due to a "cobweb of laws" in the United States (Noring 2003). The ultimate impact of this situation is that most recordings from before 1972, when a Federal law on intellectual property took effect, are effectively locked away until February 15, 2067. As a result, the project is considering relocation to Canada where other laws prevail, but the entire initiative is still private. Public organisations,

such as museums, usually lack the resources to engage in large-scale audio (or video) restoration and preservation work.

As a result, the bulk of restoration work is being done by small private companies not usually run to earn a livelihood but to invest in further "preservation work". Satisfaction for producers is largely in non-material terms, such as acknowledgement by their fellows and interactions with like-minded people. Understandably, they are not amused when others simply re-use work they have paid for without as much as acknowledgement: in the case of the Carter Family, JSP actually advertised their set as far cheaper than the more expensive Bear Family box (personal communication by Hermann Knuelle, 8 March 2005).

To be fair, the British company originally earned a reputation in its field for high quality reissues using restoration work by well-known engineers that it had paid for and was certainly pirated itself. It is only recently, that it has started ripping off others' work for issue in "value for money" boxes. Its current business model (cf. Levine 2003) probably would not function if the label had to pay for all of its restoration work. Worse still from the viewpoint of preservation, there are other labels which do not invest any money at all on original work but regularly get good reviews in periodicals and on the internet as "value for money".

Collecting societies and enforcement agencies for intellectual property rights are not interested sufficiently to take action of their own accord, presumably because there is no pressure from the major record companies. Newspapers and periodicals also see no need to concern themselves with the topic even if they are not dependent on advertising revenue from the pirates, which sometimes is the case.

Most dealers are unaware of any problems in this field and quite readily sell pirated material along with legitimate productions. Amazon, for example, shifts responsibility for infringements on intellectual property rights to its suppliers.

Consumers are obviously faced with a dilemma – the wish to buy first-class music at a low price versus the danger that supplies will dry up when producers refrain from new work for fear of being pirated or because they no longer recoup their investments. Again, the first problem is that most consumers are blissfully unaware of anything evil afoot in this field. When confronted with the facts, reactions differ from "stealing is stealing and no two ways about it", to "I'm on a restricted budget and would dearly like to buy xx if I could afford it. If I can get it at a better price on yy, why not and to hell with morals".

Producers doing restoration work would probably tolerate re-use of the work they own if they were to benefit from it, e.g.

- Through receiving credits for the work if only individual tracks are used. This might attract new customers to their productions;
- License money for re-use in other products. Again, an important condition would be acknowledgement of credit for original work.

In this way it would be possible for the specialist companies to continue their preservation work. In view of existing experience, this would not be possible without protective measures such as digital watermarks.

Bottom Line

In view of the conflicts between actor interests, a non-intrusive watermark might be the ideal solution as it does not infringe on consumer rights and enables the detection of "pirated" work produced at a grander scale, be it in the shape of physical products such as CDs or DVDs, be it in the shape of files distributed over networks. Decisions on prosecution would then be at the discretion of the victim if he wishes to prosecute genuine file sharing among friends or only practices aimed at commercial gain.

Acknowledgements

The author wishes to thank Mr. *Hermann Knülle*, a director of Bear Family records, and Mr. *Ulrich Poser*, lawyer for Bear Family in the Hamburg court case, for additional information on the court decision, including the text of the decision itself.

Sources

- Anon (2004): Bear Family gewinnt Rechtsstreit gegen Briten, Musikwoche 13/2004, available from http://www.rechtsanwalt-poser.de/doc/voe-bear.pdf
- Böhle, K. (2004): Knock out by copyright expiration, Editorial of INDICARE Monitor Vol. 1, No 3, 27 August 2004, http://www.indicare.org/tiki-read_article.php?articleId=38
- Byworth, T. (2003): Bear Family Records copyright court action. http://www.vingar.se/country/CMS-2004-03.htm
- Fraunhofer IPSI (Integrierte Publikations- und Informationssysteme): Media Security in IT http://www.ipsi.fraunhofer.de/merit/media_security/
- Levine, J. (2003): The bucks stop here; http://www.theshiftedlibrarian.com/2003/04/13.html
- Noring, J. (2003): The Project Gramophone proposal http://www.teleread.org/blog/2003_10_26_archive.html
- Schlegel, S (2004).: Die Membran-Odyssee; http://www.cinemusic.de/rezension.htm?rid=5053

About the author: *Michael Rader* studied sociology, psychology, political science and economics. He joined ITAS' forerunner AFAS in 1979 and has since worked mainly on the impacts of information and communication technologies. He has led several ITAS projects and is currently involved as workpackage leader in FISTERA (Foresight on Information Society Technologies in the European Research Area). In INDICARE, he mainly plays the role of an unobtrusive copy-editor. He has accumulated his own record collection over almost 40 years. This includes items from the beginning of the 20th century up to the present. Information on more recent DRM developments stems mainly from observation of CDs bought by his daughter.

Status: first posted 29/04/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=97

DRM and developing countries

Comments on the INDICARE state of the art report

By: Manon Ress, Consumer Project on Technology (CPTech), Washington DC, United States

Abstract: CPTech endorses the findings of the State of the Art Report. It, however, criticizes that the report focuses on Europe only, and points out that DRM is a global issue that should receive more consideration in international fora, such as WIPO.

Keywords: review – INDICARE, competition, copyright law, developing countries, fair use, privacy, transparency

The Consumer Project on Technology

The Consumer Project on Technology (CPTech) is one of the organisations that deal with DRM issues globally. CPTech, a Washington-based non-profit organisation, focuses among others on issues such as intellectual property rights, electronic commerce and competition policy. CPTech operates globally. Accredited at WIPO, the Consumer Project on Technology is actively involved in IP legislatory processes at the international level, including the negotiations about the WIPO Broadcaster Treaty and the establishment of a Development Agenda for WIPO. CPTech is also a driving force behind the Transatlantic Consumer Dialogue (TACD).

CPTech's comments on the INDICARE State of the Art Report (SOAR)

Consumer concerns in Europe have been adequately highlighted in the SOAR and CPTech supports the conclusion of Chapter 3 on consumer comcerns (cf. Helberger et al. 2004, pp. 19-43). The INDICARE report demonstrates that interests and concerns of consumers are insufficiently considered in the context of DRM-protected digital content. We would like to see, however, more considerations for consumer concerns inter-

nationally and more specifically for the weakest consumers such as consumers in developing countries. Also, an overview of international aspects of DRM and the potential impact of DRMs technologies on developing countries would be useful.

The following paragraphs will pinpoint some pressing issues in this context, paying particular attention to the matter of DRM and developing countries, but also jurisdiction issues and the role of governments and international organisations.

CPTech's opinion on pressing issues

DRM – an international discussion

DRM is being discussed in various international fora from industry led "dialogues" to intergovernmental bodies. Examples are WIPO, but also the American National Standards Institute (ANSI) the International Telecommunications Union, ITU-R Working Party 6M. Some organisations active in this field are, apart from CPTech, the Electronic Frontier Foundation (www.eff.org), the Union for the Public Domain (www.public-domain.org), the Open Knowledge Forum (www. okfn.org), IP Justice (www. ipjustice. org), Alternative Law Forum (Bangalore) (www.altlawforum.org) and the Canadian Internet Policy & Public Interest Clinic. European and US-based consumer groups such as the members of the TransAtlantic Consumer Dialogue (TACD.org) are also discussing DRMs and putting forward their concerns.

DRM – uncertainties and concerns of consumers at the international level

Consumers have expectations about how they are able to access and use content whether the content is local or global. Consumer expectations are based on practices, on how they acquire content with or without authorization (such as what has been possible so far on the Internet). Consumers sometimes feel entitled to make personal copies but often concede that some form of payment must be made. While these expectations are often shaped by the legal framework in which consumers reside, increasingly DRM technologies are limiting or excluding consumers' rights where there is no legal requirement to do so. Technologies that restrict access and use are not welcomed by consumers locally and internationally. Since many internet transactions of information goods are cross-border, it is necessary to 1) clarify existing rules and 2) examine their impact on the dissemination of information goods and innovation.

Public domain materials are a good example of documents that for most consumers are available without requiring any authorization (at least in some jurisdictions like the US). Consumers/users are not certain about the legal status of DRMs that might be used to deliver public domain materials. In some jurisdictions, it is lawful to circumvent DRMs that lock content not subject to copyright and since there are no uniform positions by rights holders or DRM providers on this issue, it creates uncertainty for consumers.

Another example is the issue of exceptions and limitations to anti-circumvention provisions: there is no harmonization among the exceptions or limitations. Consumers in different countries have different legal abilities to access and use content. Therefore a large class of users (consumers, educators, librarians, visually impaired people etc) have to accept "uncertainty" and in some cases confusing and contradictory rules to accommodate the requirements of right holders or DRM providers. If DRMs are applied indiscriminately at the international level or in a future broadcasting treaty, consumers will not only lose some of the current freedoms of access and use of content they currently enjoy, but will also experience further restrictions on the scope of limitations and exceptions. Furthermore, in the case of abuse of DRM technologies, consumers do not have access to international legal mechanisms for recourse.

The use of DRMs also raises privacy issues that seem difficult to solve at the national level. The technologies that facilitate the gathering of consumers' personal information by rights holders and DRM providers are difficult to monitor outside of one's own jurisdiction. In some jurisdictions but not others, consumers are permitted to circumvent technologies to prevent collection or dissemination of personal data.

DRM and developing countries

Regarding specific threats to developing country consumers, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) paper on TPMs and developing countries says it best: "It is no secret that DRM and anti-circumvention laws have proved dangerous to the developed world. These harms are well-documented in Canada, the United States and elsewhere" (CIPPIC 2005). DRM is dangerous to developing nations for these same reasons.

However, there are also reasons why DRM is even more dangerous to developing nations. By releasing content using DRM, foreign rights-holders may attempt to trump local copyright law and exceptions through unfair contract terms. In other words, because DRM permits consumers to access and play content pursuant to automatically-enforced license terms, contract law governs the relationship, not copyright law. Foreign rights-holders thereby bypass developing nations' copyright laws. By locking-up content in DRM, foreign rights-holders will prevent people in developing nations from accessing and using copyright works in ways that those nations' laws may allow, even for free. DRM may also prevent legal re-sale of copyright protected goods, particularly through the use of region-coding which has never proved positive for developing regions.

Further, to the extent that, like Canada and unlike the United States, developing nations are net importers of cultural products protected by copyright, DRM and anti-circumvention laws will aggravate the cultural deficit that may already exist in those countries. DRM and stronger copyright laws will have a net negative cultural and economic impact in developing nations because royalty payments to foreign rights-holders, particularly those in the United States, may increase as a result.

Finally, DRM and anti-circumvention laws could have a significant negative effect on the innovation agendas of developing nations. Developing nations depend on a technological and legal environment that fosters innovation. The American experience with DRM has shown that copyright owners inappropriately use DRM technology and anti-circumvention laws to stifle competition and create artificial monopolies. These inappropriate uses of technology and law favor bigger, established market players and artificially increase the market risk faced by smaller companies and new entrants to the markets.

Jurisdiction issues cross-border

DRMs are used to protect and deliver content on a cross-border basis. There are many legal questions that have not been answered and that need to be answered before DRMs become the international norm for protecting content.

For example: which jurisdiction and what law applies to the protection of the DRM and the content in the context of a cross-border dispute? Which country's anti-circumvention law applies to the protection or the circumvention of the DRM? The country of origin or destination? Which law applies to the use of the content protected by the DRM? Which national law would apply to the agreement regarding the delivery of the content via the DRM?

The country's law and jurisdiction may apply for acts of circumvention and for distribution (but personal jurisdiction is difficult to get if it's a foreign distributor). For online access and use, international principles are still evolving (see the Hague Project).

The question of jurisdiction is also raised in contracts. To date, there is no international agreement on which law should apply if there is no agreement between the parties of the contract. In the EU, (the Ecommerce directive) it's a "country of origin rule". In the US, each State has a choice of law principles that vary.

Again, consumers/users have no clear indication of where they stand legally which depends on where they are, where the content they want to access or use is... and how it is delivered.

In the US, we have seen some of the impact of this lack of clarity on makers and distributors of circumvention tools. For instance, non US cryptographers and security researchers have refused to post details of vulnerabilities

they've found in security technologies out of fear that they would be breaking the law in the US, and might be arrested if they visited. For example, although *Dmitry Sklyarov*'s computer program was legal in Russia, where he wrote it, according to the US Government, it was an illegal circumvention tool under US law.

Role of governments and international organizations

Right holders and DRM providers strongly believe that governments should not be involved in setting standards (for interoperability for example). However, they ask governments to ensure compliance with their private solutions and especially international solutions (the WIPO internet treaties for example were created to help industries threatened by piracy). Governments should also consider how they could cooperate at WIPO or any other international body such as UNESCO or ITU to protect "content and technologies" and "access and use".

DRM and anti-circumvention technologies have had negative impacts such as chilling academic research, stifling of innovation and increased anti-competitive and monopolistic practices. Moreover, libraries and educational institutions have found it more and more difficult to provide their services. Consumers have less choice, face increased costs for consumer goods and have expressed concerns for their personal use rights as well as privacy protection.

Today WIPO and other international bodies are examining DRMs and providing issue papers or requesting comments. For WIPO's credibility as a United Nations' agency, it is important to promote an implementation of the internet treaties that would be consistent with the development agenda goals. DRMs are controversial in the developed world and are seen as a threat to development for many developing countries. The rights holders from the North can disregard local copyright law exceptions and limitations using unfair contract terms. They can limit access or curb second hand sale or legal re-sale of copyrighted goods (which is important for developing countries). In addition, since many developing countries are mostly importers of cultural and educational goods, the increase cost will slow development efforts to increase access to cultural and educational materials. The innovation agendas of many developing countries are threatened by the negative effects of abusive DRM technologies.

WIPO can and should play an important role in ensuring that DRMs are deployed in a way that is consistent with the promotion of the arts and sciences, taking into account the rights holders and users. A fundamental task for WIPO is to make available to the member states the different choices available for implementation of treaties and their effects and potential effects.

Another important task is to deal with the disparities among exceptions and limitations at the international level. An examination of the crisis created by DRM technologies for consumers, libraries, educators, visually impaired and rights holders is necessary before new treaties containing such provisions are drafted. The impact of DRM technologies on local production of informational, cultural and educational goods for developing countries should also be examined closely.

Finally, as it is the case in the US and the EU, where there is a periodical review of implementing legislation for the so-called Internet treaties, an international body such as WIPO and/or UNESCO must collect data and review the extent to which DRMs are used cross-border and their effects on legitimate uses of information goods and innovation worldwide.

Summing up

CPTech strongly endorses the comment in the INDICARE report "currently costs seem to outweigh the benefits of DRM from a consumer point of view. Many arguments in favour of DRM either do not bear a closer examination or need time and further development until they become valid" (p. 101).

International bodies such as WIPO and its member states must 1) look for global solutions that will not harm developed and developing country consumers/users of digital goods and services and 2) set preconditions of minimum rights for consumers before

granting legal protection to DRMs. To this end, CPTech would like to see more attention being paid – in an international context – to the following issues:

1. The ensuring of access to and use of content.
2. Respecting privacy rights.
3. Interoperability.
4. Transparency.
5. Security, and that DRM software should not hamper the normal functioning of consumers computing equipment.
6. Measures against anti-competitive behaviour.
7. Clearly defined and enforceable rights for consumers, such as the right to private copy, the right to fair commercial practices, the right to be informed and refunded for faulty products, the right to privacy and data protection and the right to free speech or the local equivalent.

An appropriate framework for dealing with these issues could be the Development Agenda, which was proposed by Argentina and Brazil and on which establishment the WIPO General Assembly agreed on October 4, 2004. The Agenda calls on WIPO to focus more on the needs of developing countries.

Bottom line

It is timely and necessary for WIPO and its member states to take concrete steps to ensure that DRM technologies do not trump national sovereignty and countries' social and economic goals.

Acknowledgements

I would like to thank *Gwen Hinze*, *Cory Doctorow*, *Michelle Childs* and *David Fewer* for their help.

Sources

- CIPPIC (2005): CIPPIC Comments regarding DRM and developing nations. Ottawa 2005; http://www.cippic.ca/en/news/documents/Letter_to_Mark_Jeffrey_Feb_26_2005.pdf
- Helberger et al. (2004): Helberger Natali (ed.); Dufft Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich: Digital rights management and consumer acceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report, Amsterdam, December 2004; http://www.indicare.org/soareport
- MPI (2005):Max Planck Institute for Intellectual Property, Competition and Tax Law: International Jurisdiction(Hague Project); http://www.intellecprop.mpg.de/Enhanced/English/Arbeitsgruppen/int_zustaen_haag-projekt/int_zustaend_en.cfm
- The WIPO website, available at http://www.wipo.org
- WIPO/SCCR (2003): Standing Committee on Copyright and Related Rights: Current developments in the field of Digital Rights Management (SCCR/10/2), prepared by Jeffrey P. Cunard, Keith Hill, and Chris Barlas, August 1, 2003; http://www.wipo.org/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf
- WIPO/SCCR (2004): Standing Committee on Copyright and Related Rights: Revised consolidated text for a treaty on the protection of broadcasting organisations; Geneva, November 17 to 19, 2004; http://www.wipo.int/edocs/mdocs/copyright/en/sccr_12/sccr_12_2.pdf

About the author: Dr. *Manon Ress* is Director Information Society Projects at CPTech. Contact: manon.ress@cptech.org

Status: first posted 29/04/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=97

All in one! Volume 1 of the INDICARE Monitor for download

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: One of the deliverables of project INDICARE is a compilation of all INDICARE Monitor issues of the first year 2004/2005 in one volume. This article draws attention to the added value of this publication, shares the results of our self-assessment of the INDICARE Monitor, presents future directions, acknowledges the support by external experts, and finally asks for your support for the second year.

Keywords: announcement – INDICARE

About the INDICARE Monitor 2004/2005

The first volume of the INDICARE Monitor 2004/2005 announced here contains the nine issues which were published during the first year of INDICARE operation. It contains 62 articles written either by members of the project team or external experts. For this edition all articles have been checked again in order to diminish typos, to apply the layout rules more consistently, and to attribute keywords more carefully.

This publication has been optimized in view of its printed version. To add value we have included a *keyword index* and a *name index*. While the keyword index helps to find articles by *article-type* (editorial, interview, review, legal analysis, policy analysis, technical analysis, announcement, hands-on-experience), *subject matter* and *regional focus*, the name index references names of persons mentioned in the articles – not including deliberately names of authors. For some citing and quoting of articles might have become more convenient with page numbers. For those using the electronic version, of course searching or following active links to hundreds of sources may be more convenient than before when dealing with single issues or articles.

Note: As the present publication is basically a compilation of INDICARE Monitor issues, content has not been changed, validity of links has not been checked again, and information about the authors has not been updated.

Looking back

The main purpose of the INDICARE Monitor is to inform on consumer and user issues of DRM solutions in Europe and to stimulate public debate. Debate means two things here: first, the online-journal itself is scheduled as a platform for debate where different opinions and views can be expressed, and secondly articles posted on the INDICARE website can be discussed online straight away.

Some articles reached an audience of almost 1000 readers at our website within a month. As articles can also be obtained by RSS feed and by downloading the whole monthly issue as pdf-file, the effective readership is always larger than the counter of visits indicates. A more qualitative measure for the success and the quality of articles is the fact that articles of the INDICARE Monitor are not seldom referenced, commented or syndicated by other web resources, e.g. PaidContent by *Rafat Ali*, QuickLinks by *Richard Swetenham*, *Urs Gasser*'s blog at Berkman Center for Internet & Society Berkman Center, *Stefan Bechtold*'s blog at the Center for Internet and Society (CIS) at Stanford Law School, or at BillboardPostPlay (cf. sources).

In our view the INDICARE Monitor turned out to be among others a place,

- where empirical *consumer research* is reviewed and presented,
- where *young researchers* working on DRM can present original ideas and research,
- where interesting *interviews* with key persons in the field take place,
- where *European and US* debate meet,
- where different approaches of *value-centred DRM systems design* are presented and scrutinized, and

- where you can find information about *DRM events* which are not covered elsewhere (e.g. workshop and conference reports).

The keyword index gives an impression which topics ranked especially high. Conforming to the scope and the focus of INDICARE it is most naturally that the issue of consumer expectations, copyright law, DRMS design, business models, as well as standards and interoperability have been dealt with most often. In terms of application field, developments of online music markets were hottest.

Looking forward

For the future we want to increase the number of articles from industry stakeholders, the number of cases studies, hands-on-experiences, and critical descriptions of DRM systems. We also want to give more attention to institutional customers as consumers and users of DRM solutions, especially in the public research sector (including higher education and libraries). We also envisage broadening the European coverage of experts writing for the INDICARE Monitor, and of course we aim to make the INDICARE Monitor known more widely, and to increase our subscriber base. We would be pleased if you could be part of the solution helping us to achieve our goals.

Acknowledgments

Without the involvement of well known experts and without their stimulating contributions it would have been impossible to make our no-name start-up publication recognized as an unbiased forum of public DRM-debate. We thank the following external experts: Chris Barlas, Stefan Bechtold, André Beemsterboer, Patrick von Braunmühl, Willms Buhse, Leonardo Chiariglione, Ot van Daalen, Cory Doctorow, Thomas Dreier, Marc Fetscherin, Frederick J. Friend, Michael Girsberger, Christoph Beat Graber, Nynke Hendriks, Jan Michael Hess, Lawrence Horn, Cornelia Kutterer, Rik Lambers, Oliver Langewitz, Roy Melzer, Philip Merrill, Tihomira Nenova, Lutz Niehüser, Kurt Westh Nielsen, Bill Rosenblatt, Niels Rump, Péter Benjamin Tóth, and Cristina Vlietstra. Finally we would like to thank Gabriele Kaufmann, secretary at ITAS, for the many hours of skilled word processing and layout it took to produce this deliverable of INDICARE.

Bottom line

We invite you to get involved and to help us make the second Volume (2005/2006) of the INDICARE Monitor at least as interesting as the first one.

Sources

- Böhle, Knud (ed.): INDICARE Monitor Volume 1 2004/2005. Karlsruhe March 2005; available at http://www.indicare.org/monitor or for immediate download at http://www.indicare.org/imov1
- PaidContent: Rafat Ali http://www.paidcontent.org/
- QuickLinks: http://www.qlinks.net/quicklinks/index.shtml
- Urs Gasser's blog: http://blogs.law.harvard.edu/ugasser/
- Stefan Bechtold's blog: http://cyberlaw.stanford.edu/blogs/bechtold/tcblog.shtml
- BillboardPostPlay: http://billboard.blogs.com/

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 27/04/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=96

Editorial of INDICARE Monitor Vol. 2, No 3, 30 May 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: In this editorial we announce two new INDICARE deliverables: the first INDICARE consumer survey on digital music and DRM, and the first update of the INDICARE State-of-the-Art-Report. In this issue you will find, apart from announcing and presenting our new findings, three articles which continue the focus we started in April on DRM in the field of scientific publishing and libraries. In further articles, results of a survey addressing user perceptions of DRM systems are presented, the role of DRM systems in computer games is investigated, and two thoughtful conference reports are provided, one addressing the balance between rightholders and consumers at the international level, the other questioning consumer law in the information economy.

Keywords: editorial – INDICARE

INDICARE news

INDICARE has published the results of its representative consumer survey on digital music and DRM which was conducted in February 2005 in 7 European countries (Germany, UK, Spain, France, Hungary, The Netherlands, and Sweden) with nearly 5,000 Internet users participating. The main results are compiled in a special INDICARE Monitor article in this issue by *Nicole Dufft* who managed the survey.

We are also happy to announce the *first update* of the INDICARE State of the art report on "digital rights management and consumer acceptability" dealing with new developments since December 2004 and responding to expert comments we have received and published in past INDICARE Monitor issues.

About this issue

In this issue we continue to publish articles dealing with DRM systems in science and libraries. This time the focus covers a case study of one of the big document supply centres, the British Library. *Andrew Braid,* head of licensing and copyright compliance at the British Library explains the reasons why a DRMs had to be introduced, how it was implemented, how it works and what the current state of experience is. In an e-interview with *Tobias Steinke* of the German National Library (Die Deutsche Bibliothek) we explore the area of long-term archiving and the DRM- and copyright matters involved. The third contribution to the focus theme is from *Dan Hunter,* a professor teaching intellectual property law and cyberlaw at the University of Pennsylvania. He analyses the phenomenon of mass amateurization which means new ways of non-commercial content creation and distribution. This concept is especially interesting as it allows overcoming the simple dichotomy between legal commercial content on the one side and illegal content of the "darknet" on the other side. There is often an alternative, a third option, and that's amateur content. Hunter argues that DRM systems have to play a role in amateur content.

The remainder of the present issue contains another four articles. *Marc Fetscherin,* who already presented findings from consumer research in the INDICARE Monitor before, this time shares with us results from his own consumer survey he undertook for his PhD thesis. His findings on how technological requirements and usage restriction by DRM systems are perceived by consumers and how this should be taken into account in business strategies arouse interest in the thesis. *Danny Vogeley* who worked for INDICARE when he was at Berlecon as an intern made us aware already earlier of the dynamic field of computer games and the increasing role of DRM systems in this context. This time he introduces us to "massive multiplayer online role-playing games", MMORPG, and developments in these worlds which encourage DRM systems. Last not least, *Natali Helberger* was present at two relevant events reporting and reflecting about them. One report is on a meeting of the A2K initiative – with

A2K meaning "Access to Knowledge" – striving for a new balance between rightsholders and consumers of content giving special attention to the problems of developing countries. In May 2005 the initiative met in London to continue their work on a "Treaty on Access to Knowledge". The second conference Natali attended took place in Seattle, State of Washington, in March 2005. "Is consumer protection an anachronism in the information economy?" was the title. While the spontaneous answer to this question is of course "No", the conference report reveals that consumer protection laws may not always be the best means to achieve this goal.

Some of you will have noticed that the INDICARE Monitor appears this time last Monday instead of last Friday of the month as usual. This however is not due to a change in editorial policies, but just to a flu the editor caught. So, my apologies for the delay.

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=110

Digital music usage and DRM

Results from a representative consumer survey

Nicole Dufft, Berlecon, Berlin, Germany

Abstract: Information about the acceptance of DRM solutions by consumers is difficult to obtain, since the largest part of consumers has no, or at least no clear knowledge, of DRM. If we want to understand how consumers might benefit from or be restricted by DRM technologies, we need to learn more about the way they use digital goods and the channels through which they obtain them. The objective of the first INDICARE survey among 4852 Internet users was, therefore, to gather reliable data on the preferences and behaviour of European consumers with respect to digital goods and on their awareness and acceptance of DRM.

Keywords: survey – INDICARE, consumer behaviour, consumer expectations, consumer, music markets – EU, France, Germany, Hungary, Spain, Sweden, United Kingdom, The Netherlands

Introduction

This survey was the first of two planned surveys of the INDICARE project and was focused on digital music. This focus allowed us to ask detailed questions about current behaviour and preferences, rather than giving just a broad overview over different usage forms. The survey was conducted on the Internet in February 2005 among 4852 Internet users in seven European countries: Germany, United Kingdom, Spain, France, Hungary, The Netherlands, and Sweden. These seven countries account for about 70 % of the GDP and for 64 % of the total population in the 25 member states of the European Union (Eurostat 2005). The seven countries were chosen to cover various dimensions such as large and small countries, countries from east and west, as well as from north and south. The level of broadband penetration was taken as another decisive factor. The survey results are representative for all Internet users in the respective countries from age

10 with respect to age, gender, education and Internet usage frequency.

A large share of Internet users has experience with digital music

The results of the INDICARE survey show that large parts of the population have already gained first experience with digital music. 69 % of all Internet users have experience with music on a computer and 40 % use MP3 players. Particularly younger Internet users frequently use their computers or mobile devices to listen to music. But the older age groups also show strong interest in digital music and intend to try this new form of music in the future.

Survey results reveal, however, that digital music is not equal to downloads from the Internet. By far the most important source for digital music are CDs that consumers have either purchased themselves or CDs from family members and friends. Online music stores do not yet play a major role as a source for digital music: 29 % of the European digital music users have obtained music from online music stores, but only 9 % frequently use them.

Information about DRM and copyright is urgently needed

With digital music being so popular, one would expect that consumers have at least a basic understanding of the legal and technical foundations of digital music.

Our survey results disclose, however, that the majority of digital music users do not have the basic knowledge that seems necessary to make informed decisions. The majority of users is not well informed about the legality of their actions with respect to digital music. More than half of the digital music users either do not care whether the music they download onto their computers is copyrighted or do not know exactly what copyright means. This holds true especially for young Internet users who are at the same time the most frequent users of digital music.

The survey results also illustrate that a very significant knowledge gap about DRM exists in Europe. 63 % of the European users of digital music have never heard of Digital Rights Management, an additional 23 % does not exactly know what DRM is.

It can be concluded that significant information efforts are needed to ensure that consumers have a basic understanding of DRM, copyright, and the legal foundations for the usage of digital music. Such understanding seems necessary not only to prevent illegal behaviour, but also to defend consumer rights against possible violations.

Online music stores have to improve their information policy and customer care

The lack of information does not only concern digital music users in general but also users of online music store in particular. 79 % of the users of digital music stores did not know whether the music they purchased was DRM-protected or not. In addition, most users did not know whether any usage restrictions applied. Of those that knew about usage restrictions, the majority did not know the details of the restrictions.

It can be concluded that the information policy of online music stores about the application of DRM systems and/or the application of usage restrictions needs to be significantly improved. Online music stores that apply DRM technologies at least have to inform their customers that certain restrictions apply and how they are implemented. This is not only necessary for the sake of informed consumers. It is also necessary for the sake of satisfied customers, since a lack of knowledge about usage restrictions often results in problems when consumers want to use their purchased music files.

This is confirmed by survey results showing that about half of all digital music store users are not sure what they are allowed to do with the purchased content and have technical difficulties when using it.

Consumers are not willing to give up flexibility

The survey identifies device interoperability as the key demand of consumers. In addition, consumers frequently burn, share, and store music files. They will therefore hardly accept digital music offerings that do not support this behaviour. Commercial digital music

offerings have to make sure that their applied DRM systems support these demands of consumers. Otherwise they might lose customers to services that allow, for example, the easy transfer of files between devices or the sharing with others.

Our survey results also confirm that consumers "don't want all for free but they want value for money". The majority of users is, for example, willing to pay for music files that offer them more flexible usage rights, the ability to transfer files between devices, and the ability to share. Obviously, users are not willing to give up their flexibility in the use of digital music, even if restricted content were offered at half the price. It follows that DRM systems have to aim at supporting device interoperability and sharing features and apply relatively relaxed usage rules in order be accepted by consumers.

The Internet is an excellent tool to promote new music

Findings from the INDICARE survey also indicate that digital music on the Internet is an excellent tool for musicians and their labels to promote new works and foster sales. This is particularly true for less known musicians, since many digital music users discover new music and unknown artists over the Internet.

Even more interesting is that many Internet downloaders spend money on music after they have discovered new music: 64 % of the digital music users who have discovered a new artist on the Internet have subsequently bought a CD by this artist, 31 % have visited a concert, and 16 % have bought more digital music by this artist. The music industry should, therefore, aim at making it easy for consumers to discover new music on the Internet, e.g. by supporting sharing and recommendation features.

Older usage groups offer potential for online music stores

An interesting finding of the INDICARE survey is that older users are a very interesting target group for the providers of digital music. While young Internet users are currently the most frequent users of digital music, older age groups show strong interest in using e.g. MP3 players in the future. Digital music users above 40 download music from P2P networks less often, but purchase music from online music stores as often as younger user groups do. Older users often (more often than on average) spend money on digital music and CDs after having discovered new music.

The efforts of digital music stores should therefore not only focus on teenagers but particularly target older Internet users who are most inclined to spend money on new music. They typically care more about copyright and are better informed about DRM and legal issues than younger users.

Opinion on subscription services differs between countries and age groups

Subscription services are attractive to less than half of the users of online music stores. The opinion on subscription services differs quite considerably across countries and age groups. Subscription services are most attractive to Hungarian and French users. They are least attractive to teenagers.

We also find that the willingness to pay for music files that expire after a subscription period is limited: 80 % would rather pay 1 € for a song that they can listen to for as long as they like than paying only 20 Cents for a song that they can listen to for only a month. Accordingly, services where DRM technology makes songs expire after a certain subscription period are only attractive to a limited share of users. Providers of subscription services, therefore, carefully have to identify their specific target groups and pricing policies.

Frequent P2P users are also paying customers for the music industry

A more detailed analysis of frequent users of P2P networks reveals that the common perception of file sharers that generally do not want to pay for music is too simplified. Frequent P2P users are generally very active users of digital music, they use portable audio players or their mobile phone more often than the average Internet user does. And many of those who do not use those devices yet, consider doing so in the future.

We find that P2P users who have discovered new music on the Internet, subsequently buy CDs or purchase music from online music stores almost as often as the average digital music user does. The share of frequent P2P users who have bought music from online music stores or used subscription services over the past 6 months is even above average. We can conclude from these results that P2P users are not just free riders, but also an interesting target group for the music industry.

Highest share of frequent digital music users in Sweden

If we look at results on the country level, no consistent picture about trends in different countries emerges. Some selected results are nevertheless interesting to observe. The survey results reveal, for example, that the highest percentage of frequent digital music users can be found in Sweden. At the same time, however, Swedish Internet users have the lowest level of information on DRM and copyright.

Hungary has the highest share of users that know about DRM and has, at the same time, the lowest share of frequent P2P users. The highest percentage of frequent P2P users can be found in Spain and the Netherlands.

Internet users from Germany and the UK are most inclined to spend money on digital music: Germany and the UK have the highest share of online music store users and the highest share of users who bought digital music or CDs after they had discovered new music on the Internet.

Bottom line

Despite the popularity of digital music in Europe, most digital music users do not know what DRM is, do not know or do not care about copyright and are not well informed about the legality of their actions with respect to digital music. This lack of knowledge and awareness can have a number of consequences: First, it might result in illegal behaviour when using digital content. Second, the lack of knowledge often results in problems when consumers want to use music files they have purchased in digital music stores. And, third, when consumers do not have a basic understanding of the legitimate rights they have when using digital music, they will hardly be able to defend these rights against possible violations.

Sources

- Dufft et al. (2005): Digital Music Usage and DRM – Results from an European Consumer Survey, Berlin, May 2005; free download at: www.indicare.org/survey
- Eurostat (2005), http://epp.eurostat.cec.eu.int

About the author: *Nicole Dufft* is a senior analyst at Berlecon Research. She has been analysing a variety of ICT topics ranging from mobile computing and application service providing to DRM. Currently, she works in the field “digital consumer”. She is a member of the INDICARE project team.

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=109

The use of digital rights management in document supply

By: Andrew Braid, The British Library, Boston Spa, Wetherby, United Kingdom

Abstract: The paper, based on Braid (2004), describes the use of DRM in providing a secure document supply service; the reasons for implementation of a DRM system by the British Library; the system adopted, with reasons for the rejection of some systems; and insight into how the chosen system has been received by users.

Keywords: case study – electronic document delivery, national libraries, publishing, stakeholders – United Kingdom

Introduction

Electronic document delivery (EDD) is a relatively new addition to the older traditions of document supply and inter-library loan. EDD involves the supply of a non-returnable surrogate copy of the required item, usually an article in a journal, by an electronic method which is very fast and can be instantaneous. It has proved very popular with users who can easily obtain a copy of an article that is not held locally. This is the very reason that publishers find it unattractive. They claim that EDD permits libraries to cancel subscriptions to journals and rely on document suppliers and other libraries instead – the so called "just-in-case" versus "just-in-time" argument. Arguments to counter these claims (Russon 2001) have been met with a degree of scepticism by publishers.

These arguments have been heard for some considerable time but the recent addition of EDD to the document supply process has intensified the debate. Publishers see the possibility of users obtaining copies of articles almost at the same speed as if they were available on a local subscription. Document suppliers on the other hand see instant supply as a natural progression in the evolving nature of the document supply process. They want to be able to offer a service that does compete effectively with local supply.

One method of controlling EDD is by the use of digital rights management on the transmitted file. This article offers a background on the use of such systems and describes the implementation of such a system by one major document supplier.

Digital Rights Management

Digital Rights Management (often referred to as DRM) can either mean the digital management of rights, as in the context of this article, or the management of digital rights. The latter term, which is a market enabling technology, encompasses the identification and description of content and includes information about the rights and permissions associated with that content; usually this is done in such a way as to be interoperable with other content and access systems.

The digital management of rights means the technical protection measures that are added to (or wrapped around) a piece of content. This usually involves the use of some form of encryption and access control mechanism. As well as preventing unauthorised access, the controls limit various aspects of use of the content. Such limitations include the number of copies that may be printed, whether the file may be copied, the length of time that the file may be accessed and whether the content may be "cut and pasted". Unlike the management of digital rights, where work has been done by several organisations, for example BIC in the UK, in proposing standards for the electronic trading of rights, there is little standardization in the digital management of rights. Several systems have been developed and have found use in controlling many digital objects, typically e-books. Here the user, after downloading the necessary access software, can obtain an e-book and obtains rights using a variety of business models. Many of these are based on analogies with borrowing physical books, for instance the length of time the e-book is

available can be controlled and the item can be lent to another user.

Reasons for implementing DRM for document supply

At least three major document suppliers, the British Library, CISTI (cf. sources) and Infotrieve (cf. sources), have now implemented a method of secure electronic delivery. Although the three systems differ technically they have all been implemented for the same reason. That is because, unless such systems are in place, publishers will not grant the necessary rights for EDD to be provided.

This may seem an irrational response from publishers, nearly all of whom allow unsecured access to their online journals for subscribers and pay-per-view customers but they are unwilling to grant similar access through document suppliers. The reasons for this are that (i) publishers are not in direct control when supply is through a third party; (ii) they fear that inappropriate use might result; and (iii) as stated above they fear erosion of subscriptions. DRM systems do not provide a solution to all of these fears but they do give comfort to publishers in controlling inappropriate use.

The British Library and electronic document delivery

The British Library has experimented with several forms of EDD over the years (Braid 1993). Many of the systems described have not come to fruition, although the Ariel (cf. sources) system has been used since the late 1990's. In 2003 the Library upgraded its copying processes and replaced all the photocopy machines with electronic scanners using the Relais system (cf. sources). Although principally used for output in print format, this gave the possibility to supply any item from the collection by electronic delivery, if the necessary rights are in place. To obtain these rights it was necessary to come to an agreement with either individual publishers or their agent in the UK, the Copyright Licensing Agency (CLA). For the reasons stated above, in order to obtain the required rights it was necessary to implement a secure electronic delivery system.

The chosen system

Several forms of secure electronic delivery were investigated. All of these were based on DRM systems. Many of the early systems were rejected for one or more of three main reasons: (i) they were too expensive; (ii) they were too complicated; or (iii) they did not work properly. Trials began with one system in 2001 but it proved to be inadequate technically.

During 2002, the British Library worked closely with Elsevier to develop a system which, it was hoped, might develop into an industry standard. The Adobe Content Server and Adobe eBook Reader systems were chosen. These permit the encryption of existing PDF files in real time and allow a variety of security levels to be set. Initially, the following parameters were chosen:

- Use of the file limited to the machine on which it is downloaded;
- Printing set to one copy only;
- Saving and viewing of the article permitted, but for a limited period of time. (The time period varies depending whether the article originates from a scanned image, when the item is only available for printing for 14 days, or a digital original, when the article is available for viewing for up to three years)
- Forwarding and copying disabled;
- Annotations and conversion to speech permitted.

The other advantage was that, for users, they had software that was provided at no cost by a well known and reputable company. Many of the other systems rely on plug-in software, often supplied from very small companies. Since the initial work Adobe have integrated their eBook Reader software into Adobe Reader from version 6 onwards. This has the added advantage that, as most users already use Acrobat Reader, it is not necessary to install any additional software to use the system. However, the requirement for version 6 has caused some problems – see later.

It was also decided that rather than "push" the PDF file to the requester it would be better for the requester to 'pull' the file from a British Library server. There were several

reasons for this, but many of the problems associated with the transmission of large files as email attachments and firewalls are overcome if the requester controls the process. The drawback is that, for the standard requesting methods, the user is not online to the British Library and so cannot initiate the downloading process at the time of placing the request. However, the British Library does offer two services (Inside and British Library Direct) where the user searches and orders documents in the same online session and these will permit online delivery.

Both these services allow users to search for and select individual articles from the listing of journal content pages. Individual articles can be requested for delivery through a web interface. The British Library has agreements with some publishers for the storage and use of online journals. These publishers permit the delivery of requested articles to be online (a PDF icon alongside the bibliographic citation signifies that the article is available for immediate downloading). When such a request is placed, the PDF file is encrypted using Adobe Content Server and downloaded for viewing using Adobe Reader. The file is secured according to the parameters listed above.

For material held in paper format a different approach has been adopted. After the article has been scanned it is encrypted in the same way as above. The article is then stored on a server. An email message containing a link to the article is sent to the user. Because the security permits only the person who opens the link to download the file, it is important that the requester should be the person to do this. Thus, if the request is sent via an intermediary, it is important that the intermediary should forward the email message to the original requester before downloading takes place. An added advantage is that, as the encryption and access software is exactly the same for born-digital and scanned files, both types can be transmitted in exactly the same way.

The system in practice

The system has been operational since December 2002 for Inside users, with the name Secure Electronic Delivery (SED; cf. sources). Because of the relatively small number of documents that are available take-up was not great. Problems were also caused when Adobe changed the reader software from eBook Reader to Adobe Reader v6 in June 2003. The system linked to scan on demand from paper originals became operational in December 2003. At the time of writing (May 2005) use has grown considerably and SED is now responsible for over 10 %of all items supplied.

There are still some problems to be resolved. The main ones are:

- Some large organisations have shown reluctance to upgrade to the latest version of Adobe Reader
- Some customers who mediate requests have asked for a mechanism whereby the item can be checked to see if it is the correct item and complete before it is forwarded to the end user. At present the system does not permit this.
- There were some problems in the authentication of version 6 of the Adobe Reader software. These have been resolved with the release of version 7 of Adobe Reader

For those who have used it reaction to the system has been very positive. Many users have commented favourably on the speed of delivery and the ease of using the system.

Bottom line

The DRM system chosen by the British Library has proved to be successful. It is now responsible for over 10% of all items delivered. At first sight, the use of such a complex system for what is a relatively low-cost product may seem overkill, but it proved to be the only way that the British library could obtain the rights that it required to be able to continue to offer electronic document delivery. It is hoped that, as both publishers and users become more familiar with the use of such technology, a less obtrusive system of control might be possible.

Sources (websites current as at May 2005)

- Ariel: http://www4.infotrieve.com/products_services/ariel.asp
- Braid, J. A. (1993): Electronic document delivery: a reality at last? Aslib Proceedings, Vol 45 No 6, pp. 161-166
- Braid, J. A. (2004): The use of a digital rights management system in a document supply service. Interlending & Document Supply, March 2004, vol. 32, no. 3, pp. 189-191
- British Library SED service: http://www.bl.uk/services/document/sed.html
- CISTI Secure Desktop Delivery: http://cisti-icist.nrc-cnrc.gc.ca/docdel/sdd_e.shtml
- Infotrieve E 100: http://www4.infotrieve.com/products_services/virtual_library/e_100.asp
- Relais: http://www.relais-intl.com/relais/home/index.htm
- Russon, D. (2001): The relationship between journal subscriptions and document delivery. Assumptions versus reality: user behaviour in sourcing scholarly communication. Edited proceedings of a meeting held 25 September 2001, The Ingenta Institute, pp. 7-13

About the author: *Andrew Braid* is head of Licensing and Copyright Compliance at the British Library. He joined the former National Lending Library for Science and Technology at Boston Spa in 1968. He has held a variety of posts including management of the literature stores and reprographic unit, the conservation unit, stock relocation, building planning and service development. For the past 10 years he has been involved in negotiating licences with publishers for use of electronic journals in the Library's document supply services. He can be contacted at andrew.braid@bl.uk

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=108

National libraries, preservation and digital rights management

"The challenges of long-term preservation require continuous processes of migration and/or emulation. But the goal of DRM is to prevent exactly this"

By: Tobias Steinke, Die Deutsche Bibliothek, Frankfurt, Germany

INDICARE-Interview by Knud Böhle, ITAS, Karlsruhe, Germany. The interview explores major problems and current developments in long-term archiving and preservation trying to identify possible entry points for DRM systems in this area.

Keywords: interview – copyright law, libraries, preservation, national libraries – Germany

Tobias Steinke *is a computer scientist working at Die Deutsche Bibliothek, the German National Library. He is specialized in long-term archiving and preservation and is partner project manager of the German project kopal. Contact: steinke@dbf.ddb.de.*

INDICARE: DDB, Die Deutsche Bibliothek (the German National Library), made it recently to the news with headings like "German Library Allowed To Crack Copy Protection" (cf. EDRI-gram 2005). What exactly is the agreement about between DDB and the German Federation of the Phonographic Industry (Bundesverband der phonographischen Wirtschaft) and the German Booksellers and Publishers Association (Börsenverein des Deutschen Buchhandels)?

T. Steinke: In principle it's about our need to bypass copy protection in order to fulfil our legal obligations. The use of programs able to do so is normally forbidden in Germany due to the legal anti-circumvention rules. The urgent need behind this agreement was the fact that the German Music Archive

(Deutsches Musikarchiv), which is part of DDB, has already collected numerous copy protected audio CDs. To ensure the preservation of these CDs it is necessary to make legal copies. In principle DDB has the right to make copies, but without the agreement we wouldn't be allowed to use computer programs which enable us to effectively do so. So far we have no experience with copy protection beyond audio CDs. You can find all official information available about the agreement on our website (DDB 2005) – an English translation "The Frankfurt Group" (2005).

INDICARE: How can you ensure that the staff of DDB is skilled enough to hack and crack whatever protected content comes along? Think of a situation where circumvention-tools are not available legally…

T. Steinke: We will think about this when we get this kind of material. As a basic principle, we want deliveries without any copy protection.

INDICARE: You probably know about the agreement between KB, Koninklijke Bibliotheek (National Library of the Netherlands), and Elsevier (and other publishers) about the preservation of scientific electronic journals. In this agreement KB is clearly specified as responsible institution for long-term archiving. What are the differences and the similarities between the task and the approach of KB and DDB?

T. Steinke: First, DDB in Germany and KB in the Netherlands are the very institutions responsible for long-term archiving of *electronic* journals among others. While it is still voluntary to deposit an electronic copy at DDB (according to the present legal deposit law, i.e. Gesetz über Die Deutsche Bibliothek, DBiblG), this will change with the oncoming new law making the legal deposit of electronic copies mandatory. The proposed bill passed cabinet this month. Many publishers have already signed delivery contracts with DDB (e.g., Springer, Wiley-VCH) in this way anticipating the future legal situation.

Second, DDB has accumulated considerable experience with, for example, online theses and dissertations, while KB has gathered more experience with other materials. As both institutions have to fulfil roughly the same tasks, they are well advised to share their experiences with specific publication types to their mutual benefit. There is already an ongoing co-operation with the KB at several levels, especially regarding long-term archiving.

INDICARE: It appears as if DDB as well as KB prefer agreements on a private basis between publishers and libraries instead of a legal regulation on exemptions for libraries. I heard some library experts advocate for a legal regulation to ensure that libraries can fulfil their tasks without being dependent on bargaining power or the good will of publishers. What is your view?

T. Steinke: Your assumption is not entirely true. If legal regulations could be found representing equally the interests of all institutions involved, no further agreements would be necessary. Indeed this would be the ideal case: Legal regulations providing sufficiently clear structures. If, however, the legal regulations are not sufficient to guarantee the fulfilment of our tasks (e.g., technical protection measures must not be broken) then it is of course useful to get individual contracts with publishers or publishers' interest groups (e.g., allowing DDB to crack TPM). Realistically, in the future there'll be no way to avoid a dualism of both strategies, because the publication variance in the electronic sector is too widespread for any law to capture. Individual agreements can help to simplify the co-operation (e.g., a publisher agrees with DDB not to apply the TPM to the copies delivered to DDB). As for that, we understand the legal fixation of our rights as a clarification that helps avoiding uncertainties on both sides. That doesn't alter the need to actively seek and to intensify our contacts with publishers.

INDICARE: Let me turn to some more technical questions. I would assume that different publication types go together with rather different technical requirements for preservation. A database of online journals is one thing, while an item like an e-book is quite a different animal.

T. Steinke: We accept all file formats for publications we are obliged to collect. Currently the most common formats for electronic publications are PDF, XML, and HTML. But numerous other formats are in use, some of them are indeed very exotic. These formats complicate of course long-term preservation. Because electronic journals are mostly delivered to end-users in PDF or HTML, we get them in these formats as well. Therefore, from a technical point of view, e-journals are also single objects. We don't collect the complete presentation as it is on the publisher's site (webpage with database and shopping system).

INDICARE: As the field of scientific publishing is as international as science itself, a network of journal archives would seem more appropriate than a huge effort of one central library…

T. Steinke: Yes, definitely, and that's true from a national perspective too. There's no way for DDB to collect all available electronic publications on its own in one huge effort. We are thinking of building-up a network of reliable partners (such as regional libraries, university libraries etc.) which collect part of the publication production (not only journals but also websites etc.) in a well-defined geographical area. The collections of all these partners will then be archived at DDB without further (bibliographical) processing. By this DDB will at the same time function as backup for the partner institutions. At present we are in the state of planning this network on a national level. At the international levels discussions about co-operation and the way to chose are ongoing. With respect to web-harvesting a co-operation of national libraries and the Internet Archive (cf. sources) is already in place, however DDB has not yet joined in.

INDICARE: Well, I would have expected that international co-operation in the field of scientific publications would be most advanced. What is the state in this segment?

T. Steinke: The collecting duties and activities of a national library are normally defined by national law and target the national production of publications. Although the American Library of Congress also collects German books, this does not exempt us from our duty to collect them. Therefore co-operation among national libraries is primarily related to technical issues. We are trying to establish common technical standards and to share our different experiences.

INDICARE: Building archives for digital objects will need standards at different levels. I have heard e.g. of OAIS (Open Archival Information System) and SAN (Storage Area Network).

T. Steinke: The OAIS model is very important in the long-term preservation community. It is a theoretical model defining functional entities. It was originally developed by NASA and enhanced within the European project NEDLIB (cf sources). This model defines a terminology to ease comparison of archival systems at the conceptual level and in the phase of planning. However, the OAIS model doesn't say anything about the implementation of these systems.

SAN is a technical term of network technology meaning a specific technical realisation of storage techniques. From the viewpoint of long-term preservation, concepts should be independent of particular technical realisations, because these are constantly changing. But it's necessary to have agreements about the degree of reliability and about suitable service concepts (backup, refreshment).

INDICARE: I mentioned SAN, because *Manfred Osten* (2004, pp. 88-90) presented it in his book as a key technology to solve problems of long-term archiving by a distributed system architecture. Independent of SAN, the idea of distributed long-term archives exchanging information remains intriguing – especially when you envisage them to be used remotely by end-users all over the world.

T. Steinke: The idea of creating a shared archival system based on shared storage is, e.g. realised in the project LOCKSS (Lots of copies keeps stuff safe) at the University of Stanford (cf. sources). However long-term preservation (LTP) is not primarily about sharing documents, and sharing is not one of the main problems of long-term preservation for which we try to find solutions. A high

degree of technical skills and continuous development is needed for long-term preservation, and therefore central organisations should care about preservation and availability of committed material. These specific organisations could be understood as kind of a bank, in which you have a safe deposit box accessible for you only. A goal of our project kopal (cf. sources) is to create this kind of basis. Based on a stable technical solution of this kind we aim to develop a co-operatively usable archival system for long-term preservation. The system itself will then be hosted by a technical service provider, who is responsible for providing the requested technical competencies.

INDICARE: Digital technology blurs the border between archives and digital libraries and both may strive to offer their users *permanent access*. How should the borderline between digital archives and digital libraries be defined today?

T. Steinke: First some words of clarification why long-term preservation of electronic documents is needed and what the essential problems are. There are two problems in the field of long-term preservation: On the one hand it is about the preservation of the binary bit stream as storage technologies only guarantee duration for a limited time. Therefore service guidelines are needed to guarantee the *migration* to new storage technologies right in time. The second problem is more complex. Every file format is only usable within a given context (software, operating system, hardware). As a consequence relatively soon it will not be possible to access the content of the preserved binary bit stream. There are two concepts to address this problem. *Migration* is a process to convert a file format to another file format as long as it is still possible to interpret the source file. Of course the target file should have the same content afterwards. *Emulation* is a simulation of an old system environment needed for a chosen file on a current system. Both strategies require a continuing high effort and there is always the risk of losing some information. But it's the only chance to access any of the content in the future. A digital archive for long-term preservation should deal with these problems. A digital library on the other hand emphasises sharing and organisation of digital objects and can rely on current technologies.

There will be lots of digital libraries; nearly every institution has set up one already. Not every institution, however, has the task and/or resources to set up a digital archive for long-term preservation. True digital archives will only exist on well-defined foundations, e.g., connected to the legally defined deposit task of regional and national libraries. Most other libraries will be digital libraries which may guarantee to provide all e-publications for a limited time (~5 years). After that, digital archives – at the well-defined (higher) level – will get into place to serve as a backup (as said above) and as institutions making these publications available after a defined timeframe.

INDICARE: What happens when copyright of archived digital publications expires?

T. Steinke: Access to our whole collection is possible via the OPAC (Online Public Access Catalogue). You can use the OPAC on our webpage (http://opac.ddb.de/) or at PCs in our library. If a catalogue entry refers to an electronic resource you will get a link to the corresponding file. Depending on permissions, some links are displayed on PCs in the library only. In other words we are able to grant or cede access at any time when required.

INDICARE: Recently I heard library experts saying that libraries and archives would be willing to accept and employ DRM systems if on the other hand publishers are willing to let the libraries do their preservation job. Would you say that this kind of bargain will be typical in the future? Are there already archives with DRMS in place?

T. Steinke: As said before the challenges of long-term preservation require continuous processes of migration and/or emulation. But the goal of DRM is to prevent exactly this. Therefore a digital archive for long-term preservation is not able to preserve DRM protected material. DRM is suitable within access components for end-users.

For example, at present links to some of the objects are not shown within the web-

accessible OPAC. It would be imaginable to have an agreement with the right holders to show these links but to put some kind of DRM on them, on-the-fly during access. Note however, this process would not be connected to the archival system itself in any way. It is like fetching ware from a warehouse and sticking your label on it before selling it to the customer.

INDICARE: Is there a role of TPM and DRM in safeguarding integrity and authenticity of electronic documents stored in digital libraries and archives?

T. Steinke: Digital archives for long-term preservation should be as trustworthy as banks. Of course, within the archives techniques like checksums are used to ensure authenticity. In the end, customers of those archives have to trust in getting the "right" objects and the right content. It is the same as with books, which could be manipulated. Either you trust a library to not tear out pages or you don't. But we expect that we will have to use digital signatures for end-user access in the future.

INDICARE: A final question, more and more information is being made available by others than professional publishers forming part of our cultural heritage as well. Will this development change the task of national libraries and are they aware of the challenge?

T. Steinke: Yes, and it's a very difficult issue. Are all web pages worth being collected? What are German web pages at all? These questions are being discussed, but there are no clear answers yet. We only know for sure that we have to start collecting online publications (which we already have done), otherwise a lot of today's publications will be lost.

INDICARE: Thank you very much for this interview.

Sources

- DDB (2005): Musikwirtschaft und Buchbranche vereinbaren mit der deutschen Nationalbibliothek Vervielfältigung kopiergeschützter Werke. This press release is available at http://www.ddb.de/news/pressemitt_vervielfaeltigung.htm
- EDRI-gram (2005): German library allowed to crack copy protection; http://www.edri.org/edrigram/number3.2/library
- Frankfurt Group (2005): Press release of DDB in English: http://www.sub.uni-goettingen.de/frankfurtgroup/drms/drms.html
- INTERNET Archive: http://www.archive.org/
- Kopal – Kooperativer Aufbau eines Langzeitarchivs digitaler Informationen (Co-operative Development of a Long-Term Digital Information Archive): http://kopal.langzeitarchivierung.de/
- LOCKSS – Lots of Copies Keep Stuff Safe: http://lockss.stanford.edu/
- NEDLIB – Networked European Deposit Library: http://www.kb.nl/coop/nedlib/
- Osten, Manfred (2004): Das geraubte Gedächtnis. Digitale Systeme und die Zerstörung der Erinnerungskultur. Eine kleine Geschichte des Vergessens. Frankfurt 2004

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=107

Digital rights management and mass amateurization

By: Dan Hunter, University of Pennsylvania, Philadelphia, United States of America

Abstract: The production of culturally-valuable, expressive content is moving out of sole commercial control and into the hands of amateurs. This movement promises to provide meaningful alternatives to the commercial production of content, and equally promises to be a brake on commercial over-reaching in the DRM arena. Further, DRM has the possibility of spurring the uptake in amateur content (especially in the amateur content fields like open source and open access) by providing a simple and effective way of denoting attribution interests for the long term.

Keywords: policy analysis – amateur content, content industries, intellectual property, intermediaries, open access, open source, societal change, stakeholders, trusted computing

Introduction

Over the last twenty years we've seen extraordinary changes in the landscape of intellectual property, wrought by the speed of adoption of the general purpose computer and the internet. Even as recently as a decade ago only visionaries like *John Perry Barlow* understood that the widespread ability to reproduce and distribute digital content would change the assumptions that underpinned the music, and movies industries (Barlow 1994). He suggested that intellectual property was going to be set loose from its physical moorings, and the digital age would see the overthrow of large segments of the music, movie, and content businesses. Now, after the rise-and-fall of Napster and the rise-and-rise of bitTorrent, it is clear to everyone that the business model of established content providers is under threat. And so access control and Digital Rights Management (DRM) have emerged from the incumbent content industries as their last, best hope to control the uncontrollable spread of content that they used to be able to regulate through the architectures of cost structures and physical limits.

The war over content can, then, be seen as a fairly simple battle between file-sharers and their supporters versus the music and movie industries. This is a war fought on the battlegrounds of technology, and in the courts and legislatures around the world. But viewing it only in this way is a mistake. Focusing on this war misses the profound changes that have occurred for those who don't create content for the purpose (primarily) of commercial gain. The digital revolution makes it easy to share sound recordings; but it has also reduced the cost of creation, production, and dissemination for amateur producers of content, and the significance of these producers represent the most extraordinary change in intellectual property that we've seen in hundreds of years.

It probably has always been the case that brilliant authors, artists and creators have always been walking amongst us, unrecognized. But now these creators can produce their culturally-significant, expressive work, and send it out into the world to compete for attention with professionally-produced content. Examples abound: the eight or ten million blogs that are challenging mainstream media sources; open source software like Linux, Apache and mySQL; the open access movement within scholarly literature; the citizen journalism experiments of online newspapers like South Korea's Ohmynews; the Wikipedia, the growing list of amateur podcasters; and so on. These disparate examples represent the beginning of the amateur content movement, a movement that has been largely ignored by the commercial content industries. But this movement is quite radical, and gaining in significance.

The purpose of this essay is to sketch some issues that the amateur content movement poses for DRM, and vice versa. In the next sections I want to focus on some aspects of amateur content, and ask how they intersect with DRM. Then I'll look at the open access

and open source movements. As I'll demonstrate, the mass amateurization of content generates interesting, counter-intuitive responses to DRM.

Mass amateurization

In order to understand why amateur content is only now becoming significant, it's necessary to look at our assumptions of copyright and the way that expressive content has traditionally been generated. Copyright has played an important social role because it provides incentives to the intermediaries of the content industries – publishers, agents, movie studios, retail stores, etc. –where the processes of moving content from creator to user have been capital-intensive. These "content processes" include the creation of the content, the selection of the content for commercial publication, its production and dissemination, its marketing and its eventual use. Each of these processes has been too-expensive or too-difficult or too-specialized for amateurs to undertake. Consider magazine or book publishing: apart from the creation of the text, each stage in getting the work to market either costs money (offset printing requires large print runs, and large amounts of expensive paper), requires special knowledge (how does one request an International Standard Book Number?), or is just plain difficult (try to get a bookstore to devote shelf-space to your self-published magazine). Hence we have needed highly-capitalized intermediaries to provide these services, and this has reduced the opportunities for all but the most devoted amateurs.

But as *Greg Lastowka* and I have explain elsewhere, each of the content processes have moved into the hands of amateurs (Hunter and Lastowka 2005). With the advent of the general purpose computer - together with content-creation software for desktop publishing, music creation, film editing, and so forth - the cost of creation and production has fallen. To give you an idea, *Jonathan Caouette*'s first movie, Tarnation, was shown at the Sundance Festival. It is probably the first feature-length film edited entirely on iMovie, and it cost $ 218.32 in videotape and materials (Silverman 2004). Beyond creation and production, the internet means that distribution is effectively costless for digital content. Which leaves us only with the selection and promotion processes, which have traditionally involved expensive advertisements, and specialized marketing expertise. But recently we've seen the development of social software, which leads users to content they will like, without the intervention of marketers. An example of this is the Amazon.com feature that suggests other purchases based on the metric that "People who bought this book also bought…" This type of algorithm can suggest all manner of content that users might be interested in, based on their previously expressed preferences. This means that the amateur content-producer is no longer dependent on the highly-capitalized publisher, record label, or movie studio for selection and promotion of content.

As a consequence of all of these changes we will see the flowering of amateur content that will move directly from the creators to the users. Highly-capitalized intermediaries are no longer necessary for the creation, production, dissemination, and use of culturally-significant content. Witness the rise of blogs and amateur journalism, along with the various other examples: the band Wilco's success in its net-release of Yankee Hotel Foxtrot; the extraordinary rise of the Wikipedia; the success of web-based cartoons that do not have print syndication; and so on.

Amateurs are increasingly competing with professional outlets, even though they lack all manner of the appurtenances that we expect of content creation. They don't have paid editors, they don't have any type of "quality control" et cetera. And yet, through various means - often involving large numbers of amateurs contributing small amounts of time to the project - they manage to fact-check, manage output, and maintain quality standards as high as their professional competitors. And in areas like web-logs, open source software, and textual references works, the amateurs are beating the professionals at their own game.

DRM and amateurization

The operation of DRM within the amateur content environment is extremely interesting. Amateurs, by definition, are not in it for the money, so they have little need for access control to "protect their investment". Amateur content is therefore likely to be released without DRM; indeed it's hard to think of one amateur content provider which uses any type of access control on its content. This means that, as more and more commercial content is released with access control via DRM, we will see unlocked alternatives produced by amateurs. Consumers dislike the reduced functionality generated by DRM because they can't use the content they've paid for, in ways that they consider fair but which don't suit the content provider. The increasing reliance of commercial providers on hard forms of DRM is likely, therefore, to push users towards amateur substitutes for commercial content.

This leads to the somewhat counter-intuitive result that we might positively encourage commercial content providers to use DRM access control to lock up their content as tightly as they can, under the most restrictive terms imaginable, for as long as they want. If there were no competition to this type of locked content then we should be justifiably concerned about rent-seeking by monopoly holders, and we would see a reduction in creative activity, and a stifling of cultural expression. But as the amateur content movement progresses, competition in the marketplace for content will affect the degree to which professional providers want to offer this sort of locked content. If a record label wants to digitally-lock *Christina Aguilera*'s latest album and make it unplayable for a large number of consumers, then they should be free to do so (subject to some other policy concerns that they should not be free to break people's computers in locking their content; nor should they be able to break into other people's computers to lock their content; and so on). We can expect a range of amateur content to enter the market to compete on value, quality, and degree of access prohibition. We are likely to see two themes emerge from this. First, DRM access control in commercial content will encourage amateur content production (which is a good thing). And second, amateur content production will act as a natural brake on the imposition of over-broad access control by commercial content providers (which is also a good thing).

Thus the amateur content movement demonstrates that culturally-oriented and consumer-based concerns about DRM are (probably) less troubling than first imagined. However, two concerns remain, even if amateur content production provides some basis for hope. First, like many parts of our cultural experience, amateur content relies on the ability to reuse and remix existing material. Access control using DRM has the potential to affect the ability of individuals to engage in this type of creative reinterpretation (Lessig 2004). This point has been made before and I don't want to belabor the point again. But it is important to note that amateur content production cannot occur without the ability to use (to some extent) material which is part of our cultural heritage. To the extent that DRM stops this from happening, then we need to place limits on the ability of commercial content owners to stop amateur content reuse.

Second, the above comments about access control do not extend to its bad big brother, trusted systems computing. In trusted systems, only content signed by certain providers can be used by the computer system. An example of this is found in Microsoft's newest Media player. This type of DRM is an actively bad thing for amateur content, since amateurs are unlikely to be able or unwilling to obtain the appropriate license for their content to be used by the trusted system machine. To the extent that one thinks that amateur content is a good thing - and I think it's a very good thing indeed - trusted systems must be resisted. The market acceptance of trusted computing has been low to date, but future generations may have wider uptake. This is likely to reduce the opportunities for amateurs, and we should think seriously about changing copyright laws and using antitrust actions to ensure that amateurs retain the same access to users as multinational media companies.

Open Access and Open Source

The open access and open source movements can also be characterized as elements of mass amateurization, since they both stem from the same technological changes and they both rely on non-commercial motivations of the producers. Moreover, both movements demonstrate important lessons about amateur content and DRM.

”Open access” is the label for the principle that scholarly publishing should be freely available to everyone, without charge, political censorship, or commercial interference (Bethesda Statement 2003). The idea is, in short, to provide a publicly-accessible and useable commons of scholarly literature for everyone. “Open source”, on the other hand, usually refers to collaborative mechanisms of content production. Open source, like open access, does involve the free distribution, copying and use of creative content, but it adds the requirement that users are also free to alter the content (Open Source Initiative 2005). Open source software - like Linux or MySQL - provides the model for distributed production of complex creative objects, and the open source model has been adapted for the production of news, commentary, and many other types of content.

Open access and open source usually have no truck with DRM. Clearly the common view of DRM - that it is about access control - is inconsistent with both open access and open source philosophies. One cannot subscribe to open source or open access principles without accepting that the user is free to pass the material on to others, to read without cost, use and reuse, and so on. But as Poynder (2005) explains in an earlier INDICARE article, if one views DRM in its widest form, it is not necessarily inconsistent with open access. He makes the important point that open access authors still want to retain some rights, most notably the right of attribution, and he suggests this interest can be supported by DRM. Purists might argue that this can be achieved with digital watermarking, which is of course correct. But watermarking is a form of DRM; and this form of DRM happens to support the interests of open access.

I agree here with Poynder, and suggest that the same interest can be found in the open source movement, in the rise of amateur content generally, and in Creative Commons licenses. The vast majority of Creative Commons licenses that have been adopted to date (around 95%) require the licensee to attribute the work to its author, no matter what other conditions of use are attached. The lesson of this, and of various other examples of amateur content, is that the attribution interest is probably the most fundamental incentive of creativity in areas that are not driven by commercial concerns. It is possible then that a truly beneficial role for DRM exists in making attribution run with content, so that the author will know that her name will live as long as the content is being used.

Of course this is not the traditional view of DRM, and indeed DRM generally speaking does not handle this particularly well. While the emphasis in DRM is to remove content from use, it will be inimical to the open access and open source movements. But if one looks to the future, it is possible to suggest a beneficial role for DRM within the amateur content movement.

Bottom line

Amateur content is the elephant-in-the-kitchen of content production. It’s been around us so long that we no longer see it, even as we walk around it. In its newly visible form it promises to provide meaningful alternatives to commercial content, and equally promises to be a brake on commercial over-reaching in the DRM arena. Further, DRM has the possibility of spurring the uptake in amateur content (especially in the amateur content fields like open source and open access) by providing a simple and effective way of denoting attribution interests for the long term. We should be careful therefore to assume that DRM is always bad, and that commercial use of DRM will always trend towards over-control of the content.

Sources

- Barlow, John Perry (1994): The economy of ideas, 2(3) Wired (1994), available at http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html
- Bethesda Statement on Open Access Publishing (2003) available at http://www.earlham.edu/~peters/fos/bethesda.htm
- Hunter, Dan and Lastowka, Gregory F. (2005): Amateur-to-Amateur 46 Wm & Mary L. Rev. 951
- Lessig, Lawrence (2004): Free Culture (Penguin)
- Open Source Initiative: Open Source Definition: http://www.opensource.org/docs/definition.php
- Poynder, Richard (2005): The role of digital rights management in Open Access. The INDICARE Monitor. April 2005; http://www.indicare.org/tiki-read_article.php?articleId=93
- Silverman, Jason (2004), "Here's the price of fame: $218.32", Wired News, Jan 20 2004, http://www.wired.com/news/digiwood/0,1412,61970,00.html

About the author: *Dan Hunter* (BS LLB (Hons) LLM PhD) is the Robert F. Irwin IV Term Assistant Professor of Legal Studies at the Wharton School, University of Pennsylvania, where he teaches intellectual property law and cyberlaw. He previously taught at the law schools of the University of Melbourne (Australia), and Cambridge University (England). He regularly publishes on issues related to cyberspace law & policy, and intellectual property. He is currently researching a book on information policy for the coming era of amateur content production. Contact: hunterd@wharton.upenn.edu

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=106

Consumer acceptance of digital rights management systems

By: Marc Fetscherin, Harvard University, Cambridge, Massachusetts, USA

Abstract: This article presents parts of an empirical study undertaken by the author in respect to his PhD thesis. It deals with consumer acceptance of Digital Rights Management Systems (DRMS), with a focus in this article on the implications of the various technological and rights management requirements on consumer behavior and the demand for digital content. This article shows that there are some technological requirements as well as user rights restrictions which consumers might not accept when downloading legal content.

Keywords: survey – consumer behaviour, consumer expectations, consumer research, content industries, music markets, piracy

Introduction

Consumers have various methods, channels, and possibilities for accessing, copying, using, sharing, and providing digital content. They can either copy it illegally over peer-to-peer networks or purchase it by downloading the files from legal music providers such as i-Tunes. In that respect, content control is one of the most important aspects for content providers to fight piracy and also to successfully distribute and commercialize digital content. However, when implementing control systems, such as Digital Rights Management Systems (DRMS), it is unclear what the effects on consumer behavior are and whether consumers accept such restrictions and to what extend. It is therefore very important to understand the implications of the implementation of DRMS on consumer behavior, choices and the resulting demand for originals. The questions are: Do consumers accept specific technology requirements for legal downloads and are there any differences between technologies? Do consumers accept usage or rights requirements on digital content and are there any differences? These questions will be discussed in this article and we provide first empirical results about the

consumer acceptance of Digital Rights Management Systems in that respect.

Empirical study

The study is based on a sample consisting of about 500 students, which is a sufficiently large number to represent the wide diversity of students adequately. We got 174 responses from the anonymous web-questionnaire. Although students do not represent the entire consumer segment, they account for a considerable proportion of all consumers of these products and are part of a consumer group in which copying and sharing of digital content is prevalent. Students are also part of the group which has already been identified as being more prone to copyright violations and piracy.

Consumer acceptance of technological requirements

There are a number of technologies used by DRMS that control the access to and the usage of digital content. The respondents were therefore asked which of the various technologies used would keep them from downloading content legally. A 5-point Likert scale was used to measure the acceptability of the various technologies from a consumer's point of view. The Likert scale ranged from 1 (strongly disagree), over 2 (disagree), 3 (indifferent/undecided), and 4 (agree) to 5 (strongly agree). The question asked was: Which of the following (technological) requirements would keep you from downloading legally? The technologies to be rated were: The requirement of a username, the requirement of a password, the encryption of content, the presence of an embedded watermark on the content, the need for specific software to use the content, and the need for specific hardware. The results are provided in Figure 1, in which the horizontal line represents the various DRM technologies used and the vertical line the rating of each, represented by the median value.

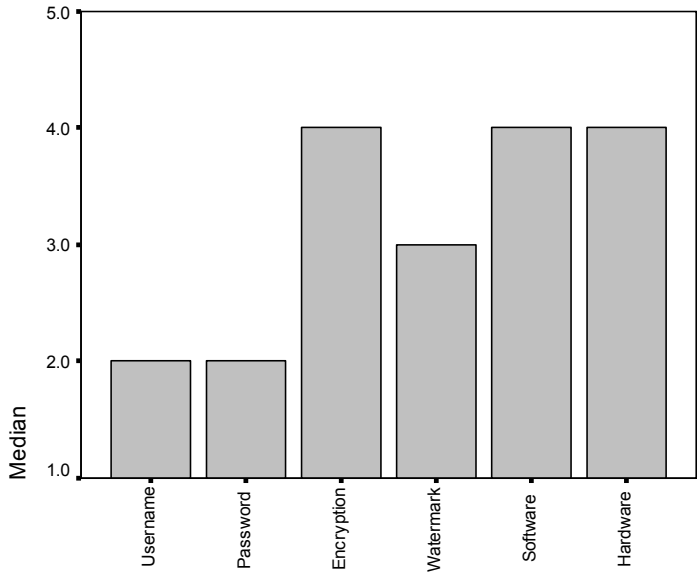


Figure 1: Technological requirements

Technologies perceived as obstacles form a consumer's perspectives are encryption and the necessity for specific software and hardware to use the digital content. The technologies not perceived as obstacles by respondents are the requirements for a username and a password. Respondents seem to be indifferent to watermarks or not having any clear idea. However, two questions arise when a Likert scale is used: Does the question measure the perception in a useful way? Second, does the scale measure what it is meant to measure? In that respect we have to conduct a reliability and validity test of the answer provided. One way to measure the reliability and validity is by calculating a Cronbach alpha. We obtained a value of $\alpha = 0.7970$, which is higher than the required $\alpha =$

0.6, indicating that the results obtained are consistent and reliable.

Consumer acceptance of rights restrictions

Content providers grant consumers various usage rights and attributes of these rights for the digital content acquired, most often expressed in a rights model. These rights can include the right to play, copy, burn, or move the content where the attributes of rights might be the number of times a song can be copied onto a CD. In most cases, they are expressed in a rights language such as XrML or ODRL. The questions arise, which of these rights restrictions and underlying attributes of rights consumers are willing to accept? Are there differences for the various rights and if so, which? We therefore asked the respondents to rate a variety of statements, each including a type of right (play, burn, and copy/move) and an attribute of that right. The question asked to respondents was: Which of the following (rights) restrictions would keep you from downloading legally? The statements to be evaluated were: Limited playability (in number), limited burning on a CD/DVD (in number), limited copying onto a PC (in number), limited copying onto mobile devices (in number), limited encoding into other file formats (conversion), and limited playability (in time). Again, a 5-point Likert scale was used to rate these statements, ranging from 1 (strongly disagree) to 5 (strongly agree). The results are illustrated in Figure 2, where each statement is outlined on the horizontal line and the median value recorded for it provided on the vertical line.

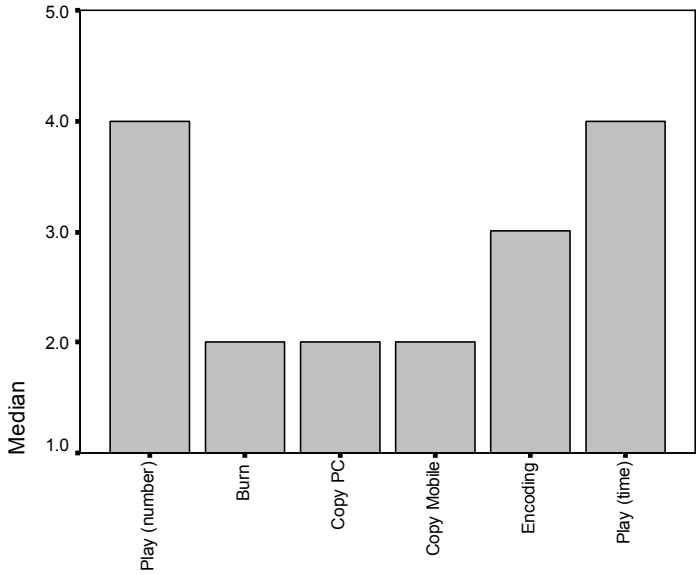


Figure 2: Rights restrictions

According to Figure 2, any restriction on playability (either in the number or in time) is not going to be accepted by consumers, as consumers perceive it as a constraint in their use of the digital content. The restrictions on the right to burn, copy onto a PC, and copy onto mobile devices are not perceived as key obstacles by respondents and might therefore be acceptable as also other studies have shown. Finally, respondents were indifferent about the possibility of converting media files from one format to another (i.e., encoding). As in the previous question, we conducted a reliability and validity test for the scale used and the answers provided. We arrived at Cronbach $\alpha = 0.8646$, which is higher than the required $\alpha = 0.6$ and thus indicates that the results obtained can be accepted as consistent and reliable.

Bottom line

Consumers have different options for acquiring digital content, either to pirate or to purchase. Thus far, the possibilities to copy or pirate for consumers, especially for music, are diverse, easy and most of the time of low risk in terms of security threats such as viruses or legal prosecution. Implementing

control systems like DRMS may make purchasing less attractive than copying for consumers as the legal products restrict them in their usage. However, the question arises which of these technologies and rights restrictions consumers perceive as obstacles and hence may reduce the utility of the original. Our results have shown that consumers dislike encryption and the requirement for specific software and/or hardware to use the digital content, and they don't like any restrictions on playability. Overcoming these obstacles may be a way for content providers to make some consumers switch from copying to purchasing, or even to make consumers switch from not consuming any digital content to purchasing it online.

Sources

- Fetscherin, M. (2005): Implications of digital rights management on the demand for digital content, Bern, 2005 (PhD Thesis, to be published)

About the author: *Marc Fetscherin* is currently a Fellow at Harvard University, at the Centre for Business and Government (CBG). Prior to Harvard, he was a visiting researcher at the University of California at Berkeley and a PhD student at the University of Bern. He holds a master's degree from the University of Lausanne and the London School of Economics (LSE). He is also a former consultant of McKinsey & Company. He is the author of many articles, book chapters, conference proceedings and presentations. He is also member of the EU expert group on DRM. Contact: marc_fetscherin@ksg.harvard.edu

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=105

Real money for virtual items: A case for DRM?

By: Danny Vogeley, Berlecon Research, Berlin, Germany

Abstract: A phenomenon in massive multiplayer online role-playing games (MMORPG) is the immense interest of players to monetize virtual items in exchange for real money. MMORPG developers do not welcome such behaviour, which has been so far beyond their control. As a result, developers are considering restricting user rights for the trade of virtual items. This article analyses DRM in a potential new role in the game market to define and to enforce developers' claimed rights to virtual items in virtual worlds.

Keywords: economic analysis – business models, consumer expectations, games, secondary markets

Introduction: Welcome to the virtual worlds of role-playing games

Digital Rights Management in the online game market usually applies to copy protection, online distribution models and online access control (Vogeley 2005). Beyond these common roles, DRM can also be used in a broader sense to manage the gameplay of virtual worlds. Especially in massive multiplayer online role-playing games (MMORPGs), the management of user rights is gaining increased relevance.

MMORPGs are persistent virtual worlds, in which thousands of players are interacting simultaneously with each other via the Internet. Each player is symbolized as a graphical representation, a so-called avatar. These virtual worlds are persistent, i.e. they continue whether an individual avatar is logged in or not (Wikipedia 2005). Usually, avatars are interacting with each other and work together in a range of different activities. The developer is in charge of supervising this virtual world to guarantee new activities and challenges for players. Users usually pay a monthly fee between € 10 and € 15 in addition to the initial purchase of the game. The

genre reaches from fantasy settings to realistic environments.

The most popular MMORPGs have more than 300.000 subscribed players. Among them are EverQuest by Sony, Ultima Online by Electronic Arts, and World of Warcraft by Blizzard. Since its release in December 2004, World of Warcraft has become one of the most successful games today. They recently announced their 500.000th subscriber in Europe (worldwide 1.5 million) (Blizzard 2005/03/17).

The trade of virtual items for real money as a phenomenon in MMORPGs

A phenomenon in MMORPGs is the trade of virtual items among the players. These items are traded via external online platforms in exchange for real money. Virtual items include coins, weapons, spells or buildings. Usually MMORPG developers did not intend this kind of trade, when they implemented transfer mechanisms for virtual items between avatars.

There is a high demand for specific and scarce virtual items, which give the owner enhanced power to accomplish further challenges. Usually, to receive such items requires much time and effort. Many players do not have the required time to "earn" these items. They simply buy the desired items outside of MMORPGs on platforms such as eBay. After a purchase, buyer and seller meet inside the virtual world to hand over the traded item.

This has led to a prosperous external market with a high monetary value for in-game items and with remarkable transactions. Recently, a player of the MMORPG Project Entropia bought a virtual island for US $ 26,500 (Lettice 2004/12/17). This purchase included mining and hunting rights, ownership of all land on the island and a castle (no furniture included). The current number one seller of World of Warcraft items on eBay has earned more than 44.000 $ each month in early 2005 (Leupold 05/06/05). Altogether, the secondary market for virtual goods is estimated at between US $ 800 and US $ 900 million annually (Terdimau 04/12/20). It is notable that players have created this secondary market by themselves.

This development has led to a big controversy among MMORPG developers about the legitimacy of these markets. Popular MMORPGs such as EverQuest, Ultima Online or World of Warcraft do not welcome external online trade beyond their control. They claim intellectual property rights to every item in their worlds and deny any real-world economic value of virtual items (Terdimau 04/12/20). Users have to comply with these assignments in the corresponding End User License Agreement (EULA).

One reason for this point of view is the increasing number of complaints from angry players, who have been defrauded by sellers. Although the developers are not responsible for these kinds of problems, their customer services are getting increasingly confronted with them. Another aspect deals with the customer life cycle: Revenue models of MMORPGs are usually based on monthly subscription fees. Therefore, developers are designing evolving worlds where users will constantly have to spend significant time to collect powerful items or to achieve higher levels. When the players can easily buy desired items outside the game, they can overcome the time needed to collect all necessary credits. This leads to reduced income for the developers. As a result, most of the largest MMORPGs have taken legal action to fight external trading. For example, the MMORPGs EverQuest and Asheron's Call forced eBay to remove every auction with items from their corresponding world (Rolston 01/01/19; Beckers 04/05/14). Blizzard is continuously cancelling accounts of players who have been identified as traders on online platforms (Klaß, 05/03/14).

DRM to control external trade of MMORPGs

However, these approaches by the developers are not sufficient to stop further trading effectively. On the contrary, the focus on eBay has led to the emergence of other less-tractable online platforms such as IGE or ItemBay.com. IGE organizes trade for more than 15 different MMORPGs and provides

an exchange rate between virtual items and real money (www.ige.com).

As a result, developers are considering using in-game tools in MMORPGs to manage the trade inside of MMORPGs more effectively (Leupold 05/06/05). Microsoft for example announced (cf. Feldman 05/03/16) that the selling of virtual items via their next-generation game console Xbox will be possible allowing the purchase of new levels, maps, weapons or skins via a one-stop-shop. This leads to a new and interesting potential role of Digital Rights Management – either to control the trade of items or to enable new business models. DRM as a tool to manage further trading of items opens up a variety of possibilities for MMORPG developers (MacInnes et al. 2004, p. 4). For example, developers can determine special rights of valuable items to prevent the handover to other avatars. World of Warcraft uses this concept on specific items: Once the item is picked-up by an avatar, it cannot be transferred to another. It is also possible to determine the maximum number of items, which can be created in a given period. DRM can also be used to demand taxes on every transferred item. On the other side, DRM can be implemented to broadly allow item trading. The MMORPG "Second Life" by Linden Lab (www.secondlife.com) gives users the right to sell items they have created by themselves.

DRM in this context is an appropriate term, because MMORPGs are not simply games, where a set of mandatory game rules by the developer applies. Rather, MMORPGs should be regarded as social spaces, where users create characters, dynamic economics, and an evolving culture (Taylor 2005, p. 4). Unlike pure computer games, MMORPGs are leading to a convergence between virtual and real life: Virtual goods do already have an economic value outside of MMORPGs and are also increasingly affecting national laws. For example, a Shanghai MMORPG gamer has killed a man in real life for selling his virtual sword (Slocombe, 05/03/31). Gradually, the boundaries between virtual and real are more and more blurred.

The role of DRM as a tool to manage, i.e. to restrict, trading is currently in its infancy. Among MMORPGs developers there is intense discussion on how to find a balance between restricting real-world exchange without limiting in-game trading too much (Ondrejka 2004, p. 2). In a widely discussed attempt by *Randy Farmer* to describe a complete eBay-resistant virtual economy, he concluded that it would lead to the removal of too many interesting features (Farmer 2004).

What the players think about the restriction of trade

Regardless whether developers are tolerating, battling or supporting the trade of virtual items, they will hardly be able to achieve consent among the majority of their customers. According to a survey by Sony among its EverQuest customers, the position for, against or neutral towards external trading is evenly split (Leupold 05/06/05). This leads to the interesting situation that one customer group would welcome the deployment of DRM to stop trade, while the other group would not. The main argument of the trade opponents is the unfairness of players paying for desired items rather than achieving them through skills and labour.

But it is likely that more and more players will be engaged in external trade and will constitute the dominant group. According to the survey by Sony, 20 to 25 % are already involved in trading. In South Korea, which has a mature MMORPG market with the largest penetration rate of MMORPG players worldwide, the vast majority is already in favour of trading (MacInnes et al. 2004).

The crucial dispute between players and developers is the question of copyright ownership of created items. Many players regard items, which they have earned or built through countless hours of game-play, as their own intellectual property with a measurable value outside the game. A survey by the Korea Game Development & Promotion Institute (KGDI) among 1.247 players of the worldwide biggest MMORPG Lineage shows that 78 % claim to own the items. Only 3 % accepted ownership of the developers (MacInnes et al. 2004, p. 9). Develop-

ers have to acknowledge the massive interest of players in monetizing their items.

Bottom line

The emergence of MMORPGs has led to an unexpected convergence between virtual and real life. MMORPG developers have to acknowledge that there is a dynamic social and economic change in their virtual worlds, which they have only partly under control. DRM mechanisms will play an increasingly important role for MMORPG developers to define and enforce claimed rights to virtual items. But in-game trading is already common practice and broadly perceived by the players as their personal right. Therefore, to balance the interests between developers and players it is crucial to adapt the increasing dynamics of MMORPGs.

Sources

- Beckers, (04/05/14): Forum post by online community manager of Asheron's Call, http://forums.ac.turbinegames.com/showthread.php?s=&threadid=8566
- Blizzard (2005/03/17): World of Warcraft sets new milestone with 1.5 million subscribers worldwide. Press release by Blizzard, http://blizzard.com/press/031705-worldwide.shtml
- Farmer, R. (2004): KidTrade: A design for an eBay-resistant virtual economy. Habitat Chronicles, PDF: http://www.fudco.com/habitat/archives/KidTrade.pdf
- Feldmann, C. (05/03/16): Analyst sees big upside in next-gen Xbox Marketplace. In: Gamespot, http://www.gamespot.com/news/2005/03/16/news_6120586.html
- Klaß, Chr. (05/03/14): World of Warcraft: eBay-Händlern droht Rauswurf, In: Golem, http://www.golem.de/0503/36932.html
- Leupold, T. (05/06/05): Spot On: Virtual economies break out of cyberspace. In: GameSpot, http://www.gamespot.com/news/2005/05/06/news_6123701.html
- Lettice, R. (2004/12/17): Property tycoon buys fantasy island. In: The Register, http://www.theregister.co.uk/2004/12/17/tycoon_buys_non_existent_island/
- MacInnes, I et al. (2004): Virtual world governance: Digital item trade and its consequences in Korea. TPRC, PDF: http://web.si.umich.edu/tprc/papers/2004/382/ppr%20Korea%2008%20TPRC%20final%20revised.pdf
- Ondrejka, C. (2004): Living on the edge – Digital worlds which embrace the real world. Linden Lab, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=555661
- Rolston, B. (01/01/19): EBay bans EverQuest auctions. In: The adrenaline vault, http://www.avault.com/news/displaynews.asp?story=1192001-94048
- Slocombe, M. (05/03/31): Legend of Mir 3 gamer killed after selling virtual sword. In: digital-lifestyles.info, http://digital-lifestyles.info/display_page.asp?section=business&id=2061
- Taylor, T.L. (2002): "Whose game is this anyway?", Negotiating corporate ownership in a virtual world. North Carolina State University, PDF: http://www.itu.dk/~tltaylor/papers/Taylor-CGDC.pdf
- Terdiman, D. (04/12/20): Virtual trade tough nut to crack. In: Wired, http://www.wired.com/news/games/0,2101,66074,00.html
- Vogeley, D. (2005): Violation of consumer rights with DRM-based usage control systems. The case of Half-Life 2. INDICARE Monitor Volume 2, Number 1, 25 March 2005, http://www.indicare.org/tiki-read_article.php?articleId=85
- Wikipedia (2005): MMORPG. In: Wikipedia.com, http://en.wikipedia.org/wiki/Mmorpg

About the author: *Danny Vogeley* is an intern at Berlecon Research. He has been analysing several digital markets like Internet broadcasting, mobile music and M-Business strategies of media companies. Currently, he works in the field "digital consumer". He is a member of the INDICARE project team.

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=104

Preparing for the Iditarod of the digital world – Bringing consumer protection into the information economy

By: Natali Helberger, IViR, Amsterdam, The Netherlands

Abstract: Is consumer protection an anachronism in the information economy? US and European experts came together in Seattle, State of Washington, US, to discuss the impact that new techniques for selling and managing electronic content have on consumers, and the role that consumer protection law should play in the information economy. INDICARE was there to report.

Keywords: conference report – consumer expectations, consumer law, consumer protection, stakeholders , transparency – USA

Introduction

Seattle was once the gateway to the gold-fields of the Yukon. Today, it was the setting for discussing the implications of a different kind of rush – the digital-content rush. Is consumer protection an anachronism in a time when vendors are rushing to explore new sources of revenues and selling electronic content to consumers? This was the theme of the conference that took place in Seattle on Friday, March 4 in 2005. Or, as the organizers themselves described the topic of the conference: "If technology can correct market failure better than regulatory intervention can, will consumer protection law be superseded by the growth of competition? Or does innovation merely create new mechanisms to exploit consumers that should be controlled with new legislation? This conference will consider the impact of technological innovation on the foundations of consumer advocacy, contracting behaviour, control over intellectual capital, and information privacy."

The organizers, among them Prof. *Jane Winn,* from the Shidler Center for Law, Commerce and Technology at the University of Washington (cf. sources for conference page) succeeded in drafting an inspiring agenda and bringing together an impressive range of excellent, mostly US but also European experts in matters of consumer protection in Seattle. The presentations pivoted around what Professor *Iain Ramsay* from York University, Toronto, Canada called the "Renaissance of consumer protection law". The speakers highlighted various consumer law issues in e-commerce. Although not specifically directed at DRM issues, the role of electronic content protection technologies for the distribution of creative content figured prominently. Moreover, one section was dedicated specifically to address the controversial relationship between innovators and consumers in intellectual property law.

Consumer protection is no anachronism in the information economy

Rob McKenna, Attorney General in the State of Washington answered in his key-note already the question that gave the conference its title. He left no doubt about his opinion that the information economy needs consumer protection law, and his intention to give more prominence to this subject matter in the future. In his opinion, technology does not make consumer protection abundant, however, consumer protection can benefit from technological developments. But the Attorney General did not restrict himself to statements; he came to Seattle with concrete suggestions. One was the suggestion to raise the budget for the consumer protection division of the State of Washington – its first budget rise since 1993. The additional resources should be invested, so said Rob McKenna, in hiring more attorneys who are specialized in technology and consumer protection matters, in the enforcement of consumer protection laws as well as in the education of consumers. Rob McKenna's assessment of the role that consumer protection law has to play in the digital economy was shared by many of the subsequent speakers. The presentations that followed also demon-

strated, however, that the devil has settled persistently in the "how" and "where".

Transparency is a controversial form of front-line defence

Even the issue of transparency – a fairly acknowledged interest in consumer protection law – and the statement that "education is a front-line defence" of consumers against fraud was discussed controversially. There was a broad agreement among participants that transparency is an essential element of facilitating the education of consumers on how to deal with digital content and how to protect themselves against fraud and disadvantageous business deals. As Professor *Pamela Samuelson*, University of California, Berkeley, pointed out, transparency is also an important instrument to stimulate competitive markets, a factor that again can contribute to enhancing consumer welfare. Professor *Glynn Lunney*, Tulane University, explained that transparency obligations can be an element not only of traditional consumer protection laws. Patent law, a form of intellectual property law, also includes elements of transparency obligations in the form of the requirement of proper attribution. The presentations and the discussion that followed revealed, however, that the opinions are still divided on how to achieve transparency, how much information consumers need and on how useful transparency actually is as an instrument to consumer protection. Professor *Thomas Rubin*, University of Pennsylvania, for example, intervened that in his opinion, the idea of using disclosure obligations to protect consumers can be inefficient for various reasons: the information provided is not comprehensible, there is too much information available, or transparency obligations pose unreasonable burdens on producers. Accordingly, he doubted, whether the increased availability of information would correct information asymmetries and thereby eliminate the problem of market failure. What consumer needed, so said Professor Rubin, was to be able to understand the essential features of competing products and select the product that offers the best terms. In other words, what consumers need in order to be effective market actors is, according to Professor Rubin, education and "wisdom". In this context, other conference participants pointed out that the effect of transparency obligations is to impose the burden of consumer protection on the shoulders of consumers themselves. In this sense, transparency obligations might be a rather convenient way for producers and service providers to rid themselves of eventual responsibilities regarding consumers (cf the reasoning in Helberger 2005).

The idea of the active consumer – an anachronism?

One issue that is at the heart of the matter is the notion of the "informed consumer", and to what extent consumers can be reasonably expected to protect themselves. Enlightening was a study by Professors *Robert Hillmann* and *Jeffrey Rachlinski* from Cornell University titled "Consumer Standard Form Contracting Practices on the Internet" (Hillmann and Rachlinski. 2001). The authors studied consumer demand as a factor to discipline market power. Informed consumers would shape markets and generate market pressure, which again would motivate businesses to offer services at fair, reasonable terms. On the other hand, the authors had to admit that the potential power of consumers does not yet play a major role in practice. One reason to explain this is that most consumers do not even read contractual notices. Only 4 % of the 92 responding interviewees generally read contractual notices and 44 % never read them. The authors concluded that transparency obligations benefited in the best case a fraction of the consumer-base – the reading consumers – and left other parties aside, such as poorer and less educated consumers. This could be an argument against relying on transparency obligations alone and in favour of taking recourse to additional, stricter obligations for service providers. The study warned, however, against lawmakers failing to take into account the cost-benefit relation of legal interference. This was also a reference to the self-healing powers of the market. In this context, Professor *Jean Braucher*, University of Arizona, introduced an interesting project - the "Stop before you click campaign". This is a campaign by AFFECT (Americans for Fair Electronic Commerce Transactions; cf. sources) to promote fair

business practices and to guide sellers, users of digital products and policymakers in developing balanced law to govern purchases of off-the-shelf software and digital products. The initiative is the result of co-operation between consumer advocates, industry representatives, non-governmental organizations and academics and has resulted in 12 principles for fair commerce in software and other digital products (cf. AFFECT).

Far away from idealizing consumer protection law

The need to approach consumer protection laws with a sound portion of critical consideration was another conclusion from this conference. Not all laws that are labelled consumer protection laws are indeed designed to take care of the interests of consumers. This was a point that was made, for example, very clearly by Professor *Norman Silber*, Hofstra University. Professor Silber demonstrated that consumer protection laws can be also pieces of rent-seeking-legislation-in-disguise, by formulating rules that respond in reality to the needs and interests of very different interest groups beside consumers. One consequence is that consumer protection rules, instead of protecting consumers, can have occasionally very detrimental effects on the position of consumers. This is not to say that there are no good and effective consumer protection laws. However, as Professor Silber pointed out correctly one should be aware of the difficulty of designing laws that respond to the real needs of consumers in an age that he described as one of "misinformation and widespread consumer victimization".

Other conference participants warned against overestimating the impact of information technologies on the position of consumers. Many problems that were identified as consumer-issues in the online sector were not new at all, but actually well-known already from the offline world. Professor *Richard Epstein*, University of Chicago, was a clear advocate of this point of view. He claimed that one result of the urge to protect consumers from the pitfalls of the online sector is that some laws contain even too much consumer protection. They are not based on a realistic assessment of who consumers are and how they behave in an information economy. The example that he gave was the Uniform Computer Information Transactions Act (UCITA), a proposed uniform law to create new rules for software licensing, online access and other transactions in computer information. Professor Epstein defended standard industry practices, such as click-wrap licenses and other standard-term contracts. However, they are target of many complaints from consumer advocacy groups (cf. AFFECT 2005b). Professor *Jean Braucher* from the University of Arizona referred to them as "sneakwrap" licenses that manipulate consumers to make purchases they might have otherwise avoided. In contrast, Professor Epstein claimed that consumer expectations actually support standard term contracts, and that such practices were economically and socially efficient.

On the question if consumer protection is a matter for general or sector-specific law

While some speakers claimed that consumer legislation does not necessarily respond adequately to the interests and needs of consumers, others demonstrated that laws that were, so far, not commonly thought of as consumer protection laws actually might serve this function rather well. This was a point Professor *Pamela Samuelson* made in her presentation. Professor Samuelson demonstrated that copyright law, which some experts claim is not designed to serve the consumer side, provides for a range of provisions that respond to important concerns of consumers. Examples brought by Professor Samuelson were the first sale doctrine, the fair use exception in US copyright law, the possibility to use ideas and information in copyrighted works and the provisions on privacy and the parental control privilege in the DMCA. Another question is to what extent these provisions are still effective in a DRM-ruled environment.

Professor *Jean Braucher*, University of Arizona, explained some of the drawbacks of general consumer protection law: most consumer protection laws still apply to products and thereby cause legal uncertainty on whether, for example, download or subscrip-

tion services qualify for protection. Moreover, often, general consumer protection law provisions are kept very general, which is another reason why they do not provide for much legal certainty. On the other hand, as Professor *David McGowan*, University of Minnesota, pointed out: using sector specific laws to protect consumer interests would also bear the risk of overstretching such laws and interpreting them too narrowly and in a biased way. This was a reason why, as Professor McGowan claimed in response to Professor Samuelson's presentation, interpreting consumer protection rules into copyright law is "at odds with basic principles of copyright law". He also pointed out that the notion of the consumer is not homogenous. Rules, such as a prohibition of reverse engineering might benefit certain parts of the consumer base; whereas the effect of the prohibition was neutral as far as other consumers, notably the group of passive or technically less skilled consumers, were concerned. This point re-emphasised another aspect that was brought forward during the conference, namely that in order to draft effective rules to protect the interests of consumers when contracting for and consuming digital content, it was crucial to know who are the consumers, and how the different segments of the market are characterized. Having said this, Professor McGowan also acknowledged that copyright law is *not exclusively* designed to stimulate creators, as already demonstrated by Professor Samuelson. He also suggested that a utilitarian view of copyright law must not preclude interpreting aspects of consumer protection into copyright law. The decisive factor, so said Professor McGowan, is the total surplus, not only consumer or service provider surplus.

Conclusions

Consumer protection is far from being an anachronism in the information economy. Consumer protection is "hot" for various reasons. There is a strong social interest in consumer protection in order to prevent social exclusion (cf. e.g. European Council 2002) and to safeguard or restore the balance between distributors and consumers of digital content. Guaranteeing a strong and independent role of consumers can be important for economic reasons, too, to promote consumers as market drivers and controlling instances. Protecting consumers in the digital economy can be hence a way to further both public and economic interests at the same time.

Still, the matter is not as simple as that. Existing consumer protection regulations are not always drafted to protect the weaker party in commercial dealings. They can also be the result of rent-seeking and industry interests. This finding further emphasizes the need to learn more about the way consumers use digital content, what legitimate consumer interests and expectations are and how they can be best protected. This is not an easy task due to the lack of homogeneity of the group called "the consumers" as well as due to the difficulty of striking a balance between sometimes rather conflicting positions, even on the part of consumers themselves. This is why the next conference to address the consumer issue should more strongly involve consumer representatives and consumer organizations. Moreover, the Seattle conference again demonstrated that consumer protection is not a legal issue only, but also a matter of adequate technical solutions and business models, thereby stressing the advantages of a more interdisciplinary approach.

One important question that needs further discussion in both the US and in Europe is to what extent consumers can be reasonably expected to protect themselves, and when a more paternalistic approach in the form of regulatory intervention is needed. On the one hand, the new technologies offer consumers new opportunities to express their preferences, to benefit from interactivity, choice and more differentiated service offers. On the other hand, factors such as the existence of technical and contractual lock-in situations, vigorous standard battles, the gap between highly educated and technically skilled and badly informed or poor consumers, render the vision of "the" consumer who is able, ready and willing to protect himself an illusion. This is why more clarity is needed on where the responsibility of consumers shall end, and where liability of service providers shall begin.

Another question that deserves future attention is whether, once it is decided that more elaborate provisions on consumer protection are needed, this is a matter for general consumer protection law, competition law or sector specific laws, such as copyright, patent and banking law. One key question in this context is whether the relevant sector specific laws, such as copyright law, are also designed to protect the consumer side and offer, among others, the procedural means to enforce the rights and interests of consumers. Also this is an issue that is far from being settled yet.

Bottom line

All speakers were well aware of the fact that most of the issues discussed that day in Seattle were not US specific problems. Currently, similar issues are on the agenda in Europe. In some fields, this was at least the impression one got from the discussion, Europe is regarded as an example when it comes to addressing consumer issues. Accordingly, there was lively interest during the conference for the way Europe is dealing with questions such as privacy, consumer policy and standardization. Many agreed with the presentation of Professor *Peter Swire* from the Ohio State University and former Chief Privacy Counselor, who emphasized the importance of comparative research and information exchange. In such an exchange, both the US and Europe could not only learn from each other but also inspire the discussion on both continents.

Sources

- AFFECT (Americans for Fair Electronic Commerce Transactions) (2005a): 12 Principles for Fair Commerce in Software and Other Digital Products, available on http://www.fairterms.org
- AFFECT (Americans for Fair Electronic Commerce Transactions) (2005b): FAQs on Uniform Computer Information Transactions Act (UCITA); http://www.ucita.com/what_faq.html
- European Council (2002): Fight against poverty and social exclusion: common objectives for the second round of national Action Plans, Brussels, 25 November 2002, http://europa.eu.int/comm/employment_social/soc-prot/soc-incl/counciltext_en.pdf.
- Helberger, N. (2005): Thou shalt not mislead thy customer! The pitfalls of labeling and transparency, INDCARE Monitor, Vol. 1, Number 9, 25 February 2005 http://www.indicare.org/tiki-read_article.php?articleId=76
- Hillman, R. A and Rachlinski, J. J. (2001): Standard-form contracting in the electronic age; available on SSRN electronic paper collection: http://ssrn.com/abstract=287819
- Shidler Center for Law, Commerce and Technology at the University of Washington: Is Consumer Protection an Anachronism in the Information Economy: http://www.law.washington.edu/lct/Events/Consumer/

About the author: *Natali Helberger* is senior project researcher at the Institute for Information Law, University of Amsterdam. She specialises in the regulation of converging media- and communications markets, electronic control of access to information and the interface between technique, media and intellectual property law. Contact: + 31 20 525 3646, helberge@jur.uva.nl

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=103

A2K: Access to Knowledge – Make it happen

By: Natali Helberger, IViR, Amsterdam, The Netherlands

Abstract: A2K stands for "Access to Knowledge" and is the acronym for a global initiative that took its start in 2004 and that is progressing quickly. The goal of the A2K initiative is to restore the instable balance between the interests of holders of exclusive rights in creative content and users of such content. One element of the initiative is the drafting of a proposal for a treaty to protect and promote access to knowledge.

Keywords: conference report – consumer rights, developing countries, disabled persons, intermediaries

Introduction

Access to knowledge – who would not agree that this is a subject matter that is of great social and democratic importance, a matter that can rightly be described as a human need, in developed as well as developing countries. Not only is access to knowledge globally acknowledged as a desirable value, worthy of being promoted and protected; there is also a widely shared feeling that in the so-called "information economy" the ongoing expansion of intellectual property law, as well as the way exclusive rights in contents are exercised, actually threatens access to knowledge in many ways. Thus it is surprising to realize that access to knowledge is an issue that has been rather neglected when drafting recent pieces of intellectual property (IP) legislation, such as the World Intellectual Property Organization (WIPO) Copyright and Performers and Phonograms Treaty, the Digital Millennium Copyright Act, the European Copyright Directive, to name but some.

The call for access to knowledge gains an additional dimension from the perspective of developing countries. As *Peter Drahos* from the Australian National University explains: "For developing countries the coming century of knowledge-based growth raises two basic development priorities. The first is that these countries must give more urgent attention to encouraging investment in human capital and this essentially translates into investment in health and education. The second basic priority is to think creatively about models of governance for the production of knowledge that maximize the participation of developing countries in the processes of innovation, that maximizes the spillover benefits of knowledge and that minimize the social cost of accumulating knowledge." In other words, the Information Society is not a phenomenon that ends at the borders of developed countries. Access to knowledge is a matter of great interest for developing countries as well, and a means to protect and defend their interests in the global economy.

Drafting a treaty on access to knowledge

In May 2005, experts from the US, Serbia, South Africa, UK, the Netherlands, Spain, Greece, Italy, Germany, Malaysia, France, India, Canada, Korea, Brasil, Chile, among others, met in London for a second round of drafting a proposal for a *Treaty on Access to Knowledge* (A2K 2005). In a two-day marathon a consolidated version of the draft Treaty was presented for discussion to representatives from non-governmental organizations and consumer organizations, academics, governments, international organizations, academics, foundations, standardization bodies and industry players.

The first meeting took place in Geneva earlier this year, when a smaller group of experts brainstormed and submitted first proposals on what the content of such a Treaty could be. The original idea for a Treaty on Access to Knowledge has its origin in a proposal for a development agenda that was made by Argentina and Brazil at a WIPO General Assembly in 2004 (WIPO 2004). Civil society representatives, among them the Transatlantic Consumer Dialogue (TACD; cf.sources) and the Consumer Project on Technology (CPTech; cf sources) recognized the potential and rightfulness of such a pro-

posal and engaged in developing it further by starting a global initiative – the A2K initiative.

Scope and content

The version of a draft Treaty that was presented in London begins with a Preamble that describes the motives and guiding principles for this initiative. The Preamble expresses concerns about an arbitrary expansion of IP rights and the effect this can have for individual participation in creation, technological and economic progress, innovation, development, research and education. The goal of the Treaty is to create opportunities for the accumulation, distribution and sharing of knowledge, as well as benefiting from knowledge on a global level. The initiative is aimed at both developing and the developed countries; it is aware of possible disparities and different needs of both, developing and developed countries.

The actual draft provisions consist of a bundle of ideas on how to promote and protect access. Most of the suggestions made have already been subject to extensive research, and are the result of practical experience or are inspired by already existing national or international legal solutions. They cover a comprehensive agenda of 12 different subject matters, all of which have in common that they address ways of how to make knowledge accessible and how to realize the economic, academic and social benefits of access to knowledge. The draft includes provisions on the nature and scope of obligations in this draft treaty, its relationship to other international and regional agreements, provisions on governance and enforcement. It has provisions regarding limitations and exceptions to copyright and related rights, on collecting societies and access to publicly funded research. Other sections deal with patents, the promotion of open standards and the relationship between intellectual property and competition law. A selection of the suggested provisions that are most relevant for the INDICARE project will be discussed more closely in the following. These are the proposed provisions concerning the exceptions and limitations to copyright law and DRMs. In a last section, an overview of the next steps of the initiative is given.

Exceptions and limitations to copyright law

One major section of the draft Treaty suggests provisions regarding limitations and exceptions to copyrights and related rights, and here more specifically exceptions and limitations to exclusive economic exploitation rights (not: moral rights). The principal idea behind this section is the need to preserve and promote a number of uses of creative works that should not be inhibited by exclusive intellectual property rights. This can be the use of works for education, science or preservation. This can be the use by groups with special needs and interests, such as persons with disabilities, but also distant education institutions, the media or developing countries. This can be the use of works by intermediaries for the purpose of making the works accessible to third parties; examples are search engines and Internet Service Providers (ISPs).

One issue that generated a good deal of critical discussion in this context was the relationship of the suggested exceptions and limitations in the draft treaty and provisions in other, existing treaties. This is most certainly a point that will deserve further attention during future meetings. Some of the proposed exceptions already exist in this or a similar form in other legal texts, such as in the TRIPs agreement or the European Copyright Directive. Others are new, such as an exception on search engines, which will be discussed more in depth in the following.

Exceptions for knowledge-intermediaries

In a vast and difficult-to-overview information environment, seekers of access to knowledge rely increasingly on the services of intermediaries that select, bundle, guide and offer access to contents. Such knowledge-intermediaries can be search engines, portals, libraries, archives or schools, to name but some. Their activity – providing access to knowledge – must be reconciled with the interests of holders of intellectual property rights to control the distribution of such content. Occasionally, the interests conflict. One example are search engines, and

the search-engine exception in the draft Treaty is a response to an ongoing discussion whether search engines, such as google.com or yahoo.com, conflict with copyright law by deeplinking and/or caching. If this was the case, holders of intellectual property rights could possibly abuse such rights to impede the function of search engines (cf. BGH 2003). The search-engine exception in the draft A2K Treaty seeks to avoid the use of intellectual property rights to impede the work of search engines. In the version from May 2005, it reads: "The use of works in connection with Internet search engines, so long as the owners of works do not make reasonably effective measures to prevent access by Internet search engines, and the Internet search engine service provides convenient and effective means to remove works from databases upon request of the right owner" (A2K 2005, article 3-1 (ix)). Additional exceptions are designed to benefit institutions that make knowledge accessible, such as education and research institutions, distant education universities, archives and libraries.

The exceptions in favour of knowledge-intermediaries such as search engines, libraries, archives and academic institution acknowledge that one important precondition for access to knowledge is the existence of institutions that make knowledge accessible. Consequently, one way to stimulate access to knowledge is to support the work of institutions that generate, aggregate and disseminate knowledge. The experts at the London meeting remarked rightly that the work of such institutions should not stop at national borders. It was demonstrated that there can be valid, also economic, arguments to open for examples archives in one country for citizens in other countries. Share-as-share-likewise models can be the basis for sustainable and attractive business models and, at the same time, ensure that citizens from different countries have access to knowledge hosted in other countries.

In a similar direction – making knowledge accessible – are provisions in the draft Treaty that seek to expand and enhance the knowledge commons. Proposals made include the compulsory licensing of copyrighted works in developing countries, the making available publicly of works resulting from government-funded research, access to archives of public broadcasters and government information as well as the idea of so-called "Knowledge Commons Databases". The proposed Article on Knowledge Commons Databases stipulates that persons, organizations or communities that seek to establish open databases that address an important public interest and are freely available to all should be exempted for a limited period of time from the application of exclusive rights.

Exceptions for people with special needs

Accessibility is also at the heart of a set of exceptions in favour of visually impaired or hearing impaired persons or persons with other disabilities. A representative of the World Blind Union explained the special situation of these groups. Two major issues in this context are accessibility and equity. People with visual, hearing or other impediments should be able to read same material as everybody else at the same time. This means in most cases that the content has to be adapted beforehand. Where the exercise of economic rights in contents inhibits the making larger of, reformatting and offering of contents in a format that is compatible with special player devices, this goes clearly at the expense of people with disabilities. To improve this situation, exceptions are needed that allow the formatting of works and also the importing and exporting of works that have been already formatted in another country. The international availability of accessible content created in one country should not be restricted because different exceptions apply in different countries. This is even more so because the amount of adequately formatted material is limited. Important was also the observation that there is no homogenous group of disabled people and that each group would need its own specific set of exceptions in order to be able to benefit from access to knowledge. The representative of the World Blind Union emphasized that the different groups of disabled people have a strong interest in stimulating large commercial production of readable copies and are therefore interested in active cooperation

with publishers and in finding ways to reconcile the interests of all parties.

Access to knowledge and digital rights management

Article 3-6 of the draft Treaty is specifically directed at Digital Rights Management (DRM) and Technological Protection Measures (TPM) that are designed to restrict electronic access to knowledge. In its first part, the proposed article points towards the risks of DRMs and/or TPMs for the application of exceptions and limitations to exclusive rights, access to knowledge for the visually impaired or other people with disabilities, consumers, competitors and archives. The provision warns that unfair contract terms, the so-called business rules that are enforced through DRMs and the inadequate disclosure of limitations of uses of works can harm consumers. It, furthermore, calls attention to the danger of anti-competitive practices as a consequence of the use of DRMs or TPMs. Market segmentation and anti-competitive tying practices may result in higher prices and reduced innovation. The present wording of the draft provision acknowledges that DRMs are part of a larger problem that reaches into the realms of competition law and consumer protection. Having said that, several experts criticized that the provisions on consumer protection were still too narrow and required more elaboration, possibly in a separate article.

The goal of the second part of Article 3-6 is to ensure that the users of DRMs or TPMs respect prevailing public interest reasons in making knowledge accessible. The present concept of the second part of Article 3-6 of the Treaty to realize this objective is to say that legal prohibitions against anti-circumvention of DRM and TPM measures shall be restricted or not enforced in certain cases. Examples are a situation in which DRMs or TPMs preclude the implementation of Free and Open Software, in which the operators of such measures fail to inform consumers about their restriction modes and the terms under which they can be invoked or where DRM and TMPs are used to restrict access to public domain material. Insofar, national regulations should not prohibit the making available of technologies or services that facilitate circumvention for legitimate or authorized uses. One of the criticisms that were expressed regarding this proposal is that only few consumers will have sufficient confidence in their technical abilities to actually circumvent DRMs and TPMS. Another problem is communicating clearly and understandably to consumers when they would be entitled to do so.

Bottom line

As one participant worded it: “Our strength is diversity, our weakness is too much diversity”. No doubt – the Access to Knowledge Treaty is an ambitious initiative that seeks to cover a whole range of areas. The resulting danger is to loose sight of the ultimate goal and to get caught in a multitude of different topics each of which might deserve to be subject of an initiative of its own. But this is just one reason more to remember the strength of the A2K initiative: this is the ability of its initiators to mobilize a group of international experts from different disciplines and backgrounds that all share a common motive: being convinced that it is high time for some action to restore the often deplored imbalance between consumers and producers of electronic content. The composition of the round of experts that came together in London enabled the scrutinization of this first proposal from many different perspectives and its exposure to constructive criticism from different disciplines and areas of expertise.

The present content page of the draft reads like the wish list of someone who has missed out the last three year’s Christmas. It gives a good impression of the range of issues that have been, on the one hand, caused and, on the other hand, ignored by recent legal, economic and technological developments in the IP field. It is now for the drafting committee(s) to extract from this pool of ideas the most relevant ones and to expose them to further discussion. For the time being, the participants in the second A2K meeting left London exhausted but with the distinct feeling of having taken yet another step in the right direction.

Sources

- A2K (2005): Draft Text of the Access to Knowledge Treaty, available on: http://www.cptech.org/a2k/consolidatedtext-may9.pdf
- Agenda of the A2K meeting in London, available on http://www.tacd.org/docs/?id=269
- BHG (2003): German Federal High Court of Justice (Bundesgerichtshof - BGH), decision of 17 July 2003, No. I ZR 259/00 (Paperboy), in: GRUR 2003, p. 958
- Consumer Project on Technology (CPTech): http://www.cptech.org
- Transatlantic Consumer Dialogue (TACD): http://www.tacd.org
- WIPO (2004): Proposal by Argentina and Brazil for the Establishment of a development agenda for WIPO, WIPO General Assembly, Thirty-First (15th Extraordinary) Session, Geneva, September 27 to October 4, 2004, available on http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=31737

About the author: *Natali Helberger* is senior project researcher at the Institute for Information Law, University of Amsterdam. She specialises in the regulation of converging media- and communications markets, electronic control of access to information and the interface between technique, media and intellectual property law. Contact: + 31 20 525 3646, helberge@jur.uva.nl

Status: first posted 30/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=102

First supplement of the INDICARE State-of-the-Art-Report released

By: INDICARE Team

Abstract: The issue of DRMs and Consumer Concerns is beginning to draw attention. This is one conclusion of the first supplement of the INDICARE State-of-the-Art Report. After the INDICARE State-of-the-Art Report, published in December 2004, has provided a first overview of the social, technical, legal and economic discussion about Digital Rights Management (DRM) solutions, the INDICARE-team continued to monitor the developments in this sector. The present supplement reports on new developments since December 2004. It also responds to a number of comments INDICARE received on the first report from experts and interested parties. Central in the present publication is a selection of issues that reflect new developments or that, in the view of the INDICARE team, deserve more attention in future discussions.

Keywords: announcement – INDICARE

Topics that this publication reports about are, among others, the authorized domain, recent studies concerning the position of consumers with disabilities and DRMs, developing countries, and international aspects of DRM in general. The supplement describes recent legal initiatives in Norway, Germany and Belgium. It also highlights some important consultation procedures and initiatives concerning DRMs that were initialised by the European Consumer Law Group (ECLG), The European Consumer Organisation (BEUC) and the Transatlantic Consumer Dialogue (TACD). An update on recent technical developments in the field of copy protection for different media is given. Finally, the role of DRM in the information economy is discussed and if DRM, from the business perspective, are primarily means of copy protection or business model enablers. New DRM-based business models are introduced that are based on viral marketing, peer-to-peer networks or subscription and rental services. And then there are alternative business models, new DRM-free content offerings that are reported about in this supplement.

The supplement concludes that the DRM sector is on the move, and that consumer and DRM issues are slowly but consequently

generating more attention and triggering new initiatives in research, business models, and on the regulatory field. The authors conclude: "The issues discussed in this publication are issues that will very likely see more activity in the future. INDICARE will continue to monitor the sector until the next update end of the year".

The first supplement to the State-of-the-Art Report on "Digital Rights Management and Consumer Acceptability. A Multi-Disciplinary Discussion of Consumer Concerns and Expectations" is available for free **download** at: http://www.indicare.org/tiki-download_file.php?fileId=111

You are kindly invited to give us your feedback, please use the "add comment" button below. Your feedback will be considered in a second update of the report.

Status: first posted 27/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=101

INDICARE consumer survey on digital music published

By: Nicole Dufft, Berlecon, Berlin, Germany

A representative survey among 4852 European consumers finds that a large share of Internet users already has experience with digital music. However, the survey shows that the main source for digital music are ripped CDs, not Internet downloads. In addition, the survey reveals that consumers are not well informed about usage restrictions and DRM applied by online music stores. As a result, they are confused when technical restrictions keep them from burning, sharing or transferring music between devices. The report also shows that digital music on the Internet is an excellent tool for musicians and their labels to promote new music.

Keywords: announcement – INDICARE

According to the survey that was produced by Berlecon Research for INDICARE, 69 percent of European Internet users listen to digital music on their computer, 40 percent use a MP3 player. Digital music files are, however, not primarily downloaded from the Internet. By far the most important source for digital music are ripped CDs that consumers either purchased themselves or borrowed from family members and friends.

Already one third of digital music users have shopped in online music stores. Their experiences, however, were not always good ones. The majority of music store customers is not well informed about usage restrictions and the application of Digital Rights Management (DRM) technology. "This lack of knowledge often results in problems when consumers want to use their purchased music files", says Nicole Dufft, senior analyst at Berlecon Research. "Consumers expect that they can burn, share, and transfer their digital music files between different devices. They are confused and annoyed when technical restrictions keep them from doing so." Berlecon, therefore, recommends online and mobile music stores to significantly improve their information policy. "This is not only necessary for the sake of informed consumers but also for the sake of satisfied customers."

The survey results confirm that music on the Internet is very well suited for marketing activities by musicians and their labels: 64 percent of the digital music users who have discovered a new artist on the Internet have subsequently bought a CD by this artist, 16 percent have bought more digital music. This should be reason enough for the music industry to make it easy for consumers to discover new music on the Internet, e.g. by supporting sharing and recommendation features. The report also reveals that these efforts should not only center around young user groups but

should particularly target older Internet users. Nicole Dufft: "We found that particularly those older than 40 have spent money on digital music and CDs after having discovered a new artist."

The representative survey was conducted in February 2005 among 4852 Internet users in Germany, UK, Spain, France, Hungary, The Netherlands, and Sweden. The survey is part of the INDICARE project, which aims at raising the awareness about consumer and user issues of DRM solutions in Europe.

The survey results are available for free download at www.indicare.org/survey.

Status: first posted 24/05/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=100

Editorial of INDICARE Monitor Vol. 2, No 4, 24 June 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The nine articles of this issue (one of them an interview) are arranged in a topical order *regulation (4)*, *business* (3) and finally *technology* (2) – knowing of course that in DRM matters all three dimensions are concurrent. Two articles appear to be especially suited to provoke and raise debate: One severely criticises the CC approach ("Creative Humbug") and the other ("Contractual balance in digital content services") investigates the far reaching implications of the long-term shift from a product paradigm to a service paradigm in digital media offerings. In the new setting, DRM systems would no longer be understood as restrictions by consumers but as part of a fair bargain.

Keywords: editorial – INDICARE

INDICARE news

The *3rd INDICARE Workshop* about "Fair DRM Use" was organized by the Institute for Information Law (IViR) and took place in Amsterdam, 28 May 2005. The findings of the workshop and the papers presented will be made available as "workshop report" next month.

The *first INDICARE survey* on "Digital Music Usage and DRM" published end of May has been downloaded more than 1,000 times in one month. An invitation to present the survey results at Jupiter's DRM Strategies Conference (cf. sources) in New York next month is another indicator that INDICARE's European consumer survey has raised interest.

About this issue

Regulation and confusion

We start this issue with an INDICARE-Interview by *Nicole Dufft*. She interviewed *Till Kreutzer* of iRights.info (an information portal aiming to help consumers with copyright law in the digital world). The interview is particularly interesting because the criticism of current copyright law is not derived from sophisticated academic debate but based on complaints and lack of orientation felt by consumers. On the one hand copyright law becomes more and more relevant for consumers, on the other hand it gets more complex and more confusing. More information is one answer, the other is to rethink copyright.

Péter Benjamin Tóth, a copyright expert, who has also argued in this journal before to rethink copyright (Tódt 2005) is this time very polemic about Creative Commons, accusing CC licenses of being inflexible and unenforceable at the end of the day. In the context of an informed dialogue (i.e. INDICARE) it is not the polemic that counts, but the issue raised. What is at stake is, so to speak, the "standing" of CC licenses. CC advocates are of course invited to counter Tóth's arguments and allegations.

In the next contribution CC advocate *Ellen Euler* (Centre for Applied Legal Studies, Karlsruhe) argues that to be successful, Open Access requires open content licenses like Creative Commons Public License, Science Commons Public License or – relevant in Germany – Digital Peer Publishing License. The state and role of CCPL, DPPL, SCPL in scientific open access publishing is presented and discussed. In her view, most authors still do not make their works openly accessible simply because they are not informed – not because of shortcomings of licenses available.

The article by *Thomas Rieber-Mohn*, University of Oslo, addresses the implementation of the EUCD Article 6 in Norway. He argues that the approach taken in Norway contains innovative elements and would offer real protection of consumer rights – presumably more than in any EU member state. Isn't it amazing that a non-EU-country is going to implement the EUCD in a more consumer-

friendly way than any EU member state? Let's look again after the law has passed.

Business models and emerging media markets

The "business section" of this issue is opened by *Timo Ruikka* (Nokia). In a type of foresight exercise, he presents the move from media *products* to new media *services*. In these new media services DRM has another role to play than in the old "legacy model" of book and CD purchases. Ruikka believes that these future DRM-based services (e.g. lending, rental, "disposable" consumption of works) will provide significant value to consumers. In this future setting "contractual balance" will become more relevant.

Philipp Bohn, a new colleague in the INDICARE team working for Berlecon, introduces himself as an analyst with two contributions. In his first contribution he analyses new music offerings on a subscription basis by Yahoo!, RealNetworks and Napster – not yet the future services Timo Ruikka has in mind. Bohn investigates the different business models, the features of the DRM systems applied, and the advantages and disadvantages respectively for consumers, online retailers and the music industry.

In his second article he elaborates on the hypothesis that commercialization of P2P sharing offers potential benefits for consumers and the industry alike – a topic first dealt with in the INDICARE Monitor by *Bill Rosenblatt* (2004). Philipp Bohn analyses again different business models and evaluates what's in them for consumers and businesses. Both articles also add to the findings of the first INDICARE survey (cf. the article by *Nicole Dufft* in the last INDICARE Monitor). While the survey gathered reliable data on the demand side, i.e. on the preferences and behaviour of European consumers, the present articles add information not readily available about the supply side (in particular P2P- and subscription based services).

Technical matters

The last two contributions deal upfront with technical matters, however they also touch upon the future of DRM-standardisation and new application fields. *Ernő Jeges* from SEARCH, our Hungarian partner, first describes the Digital Media Project (DMP) giving a brief overview of DMP and its approach. Although we already published an interview with *Leonardo Chiariglione* last year (Chiariglione 2004), we have decided to deal again with this project, because DRM-standardisation is one of the crucial issues, and DMP offers one bottom-up approach to DRM-standardisation worth following, analysing and assessing. What we publish in this issue is just the first part. The second part will go a step further, attempting to assess the DMP approach in order to stimulate debate about its merits and possible shortcomings, and more generally about practices of DRM-standardisation.

Finally *Ernő Jeges* reports about a three day course on "Digital Rights Management – from theory to implementations" organized by the Université catholique de Louvain (Belgium). In fact it was an expert meeting about different technical aspects of DRM. The report however is not only interesting for engineers. The course also produced insights into future application fields of DRM like 3D object representations, 3D-television, 3D-Google or digital cinema, all of which seem to deserve technical protection measures not yet developed.

Bottom line

This present issue is particularly full of thorough analysis and provocation. Why not use the comment function of the articles on our web-site?

Sources

- Chiariglione, Leonardo (2004): Chiariglione's vision: An interoperable DRM platform to the benefit of all. INDICARE-Interview by Knud Böhle INDICARE Monitor, Vol. 1, No 6/7, December 2004; http://www.indicare.org/tiki-read_article.php?articleId=58
- DRM Strategies Conference in New York, July 27-28: http://www.jupiterevents.com/drm/fall05/index.html

- Dufft, Nicole (2005): Digital music usage and DRM. Results from a representative consumer survey INDICARE Monitor, Vol. No 3, 30 May 2005; http://www.indicare.org/tiki-read_article.php?articleId=109
- Rosenblatt, Bill (2004): Learning from P2P: Evolution of business models for online content. INDICARE Monitor, Vol. 1, No 6/7, December 2004; http://www.indicare.org/tiki-read_article.php?articleId=61
- Tódt, Péter Benjamin (2004): Need for a comprehensive re-thinking of "DRM" systems and copyright INDICARE Monitor, Vol 1, No 9, 25 February 2005; http://www.indicare.org/tiki-read_article.php?articleId=79

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 27/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=120

Copyright – complexity – confusion

"The basic approach to copyright needs rethinking"

By: Till Kreutzer, iRights.info, Berlin, Germany

INDICARE-Interview by Nicole Dufft, Berlecon Research, Berlin. Copyright has become increasingly complex and difficult to understand. Consumers of digital content as well as content creators are confused about their rights and obligations arising from copyright law. Better information of users of digital content is necessary, but at the end of the day the basic approach of copyright needs rethinking.

Keywords: interview – consumer behaviour, copyright law, creators, file sharing, private copy, transparency – Germany

About iRights.info and Till Kreutzer

Is private copying a crime? Is it illegal to copy a CD or DVD? Or to save a movie to my computer's hard-drive? To answer these questions is more difficult than ever, as changes in copyright law result in a complexity that is hard to oversee even for lawyers – let alone for common users. iRights.info, a new German information portal for copyright law in the digital world, wants to give users orientation.

Till Kreutzer is editor of iRights.info. He is a lawyer and partner in the "Office for Information Law Expertise" in Hamburg. He is heading the copyright division of the "Institute for Legal Issues on Free and Open Source Software" (ifrOSS) and was a member of the working group of the German government for the reformation of the German copyright law (the so-called "second basket").

INDICARE: Mr. Kreutzer, why is copyright becoming increasingly complex and difficult to understand in the digital world?

T. Kreutzer: The reasons are manifold. In my opinion there are two main causes for the increasing complexity of copyright law for the consumer. First, copyright causes new problems for the consumers simply because it concerns them increasingly. In the "analogue age" copyright was of minor importance in private life. Reading a book or listening to a record does not pertain copyright so there was no need for the user to care about legal issues when using intellectual goods in the usual way. This even applied to private copying. The few (technical) possi-

bilities to make private copies like photocopying an article in a library or recording a broadcast with a video recorder were indisputably permitted by (German) law.

The coming of digital technologies introduced essential changes in the possibilities for the user to handle copyrighted goods and in consumer habits. All of a sudden everybody was able to become a distributor and creator of copyrighted works with his home equipment – a normal personal computer was enough. It seems that still even today most users don't accept or don't understand that when using the Internet one has to be more aware of copyright issues. There are significantly stricter rules when publishing on the net than for any use in the private environment. For example most users don't seem to understand that they need permission when publishing other peoples' works on the Internet even if they don't pursue any commercial interests. Apparently users think putting pictures or texts on the Internet is comparable to sharing CDs or videos with friends. It is apparently hard to understand for the users that in terms of copyright law the salient point is not the lack of commercial purpose but the making available to the public.

The second reason for the increasing complexity of copyright law for the consumer is a result of copyright law itself. The modification of existing copyright exceptions, the complexity of the new exceptions and the legal protection of technical measures like copy protection and what that means for private copying have led to profound problems of understanding. This happened because the legislator had to make significant compromises in the face of the massive lobbying of the various stakeholders. To give an example: In 2003 the German legislator introduced a new copyright exception that allows the online use of copyrighted works for educational and scientific purposes. Due to substantial lobbying of the film industry, among others, this exception was restricted in regard to motion pictures. This means that movies are not allowed to be used in schools or universities unless two years have passed since their first performance in the cinemas. What the legislator did not consider was that many films, especially those that are of peculiar interest to education and science, are never shown in cinemas, for example documentaries and educational films. The legal position regarding these films, which are indisputably numerous and significant, is completely vague. Teachers would have to be copyright experts in order to be able to decide if the 2-year rule can be applied to these kinds of films as well.

INDICARE: What are, in your experience, the major problems that consumers of digital content are facing today? What are the most common topics discussed in your forum? Where are information gaps most severe?

T. Kreutzer: In my experience, the biggest uncertainties exist in relation to the private copy exception (which is mandatory under German law) and the protection of technical measures (technical copy protection). Both the reasoning behind the legal solution and the legal provisions in detail leave open a large number of questions.

For example it is difficult to explain why the lawmaker decided that digital private copying is still legal but, at the same time, it is illegal to circumvent technical provisions to make the copy. The users - who are generally not familiar with legal issues - seem to think this is a semantic error.

However, there is even more to it: most users are highly alienated by the anti-circumvention rules in general. In my opinion the reasons are obvious. The term "circumvention" for example is so vague that even experts don't know what it exactly entails. The possible cases are so various and widespread that many questions remain open – even if one does have an idea about the legal issues. Is it illegal to copy a CD that is labelled "copy protected" by using an ordinary CD recorder and ordinary copying software? Am I allowed to make a record of a protected music file by analogue copying? Is it allowed to circumvent CSS when otherwise I would not be able to watch my DVD on my Linux laptop? These are all frequently asked questions. On the one hand it is understandable that the legislator utilized so many vague terms in order to make sure that the law will not be obsolete by the time it is enacted. On the other hand it leads to insur-

mountable difficulties when attempting to apply this law, specifically for the normal user.

Another point of insecurity for users pertains to questions of filesharing. We have observed that most users assume that "filesharing is illegal". I emphasise this exaggerated, undifferentiated statement intentionally because it reflects the misconceptions regarding copyright very well. Even fairly "informed" users are not aware of the difference between file-downloads, that are in most cases permitted according to the private copying exception, and the provision of files on their harddrive for others. For users both acts are directly related. This perception can be traced back to the technical environment. In general the default settings of the filesharing client software are set up in a way that every downloaded file will be saved in the "shared folder" which means that it is automatically made available for other users to download. I suppose that most users don't even know that the default settings of their filesharing software can be changed in order to prevent the distribution of their files if they made up their mind to do so.

The uncertainty about private copying was increased by the amendment to the German copyright act in 2003. In the course of this reform the German legislator adopted a restriction that prohibits even the download (or any other form of private copying) from another filesharing user if the source file (i.e. the file on the other user's computer) was "obviously illegally created". The legislators' intention was to prevent illegal copies of protected works from lawful circulation. The new rule is directly aimed to stop downloading in filesharing systems. But the bottom line is that the restriction is useless because in the vast majority of cases the downloader has no possibility of knowing under which legal circumstances the source copy was made. After all, the source might be a (legal) private copy, an original or even produced in a copyright haven, i.e. a country where no copyright is granted. Against this background there is a serious disparity between the uselessness of this rule for the rightsholder to prevent illegal copying and the debilitating uncertainty it raises for the users.

Let me add one point: These observations take into account that our (iRights') users are quite likely already somewhat informed and already have a clue about copyright issues. The level of awareness of other consumers is pure speculation.

INDICARE: Your portal also addresses creators of content, such as artists, musicians, journalists and producers of amateur content. What are the major challenges they are facing with respect to copyright issues? What are the opportunities for creators?

T. Kreutzer: In our experience, many content creators are confused about their rights and obligations arising from copyright law. Information technology and digital formats make it possible to extract parts of existing works and to rearrange, recombine and readapt them in order to create new work. This technical environment produced new art forms, which came up primarily in the realm of music, for example Hip Hop, electronic music and club music. But film making changed also with the new digital tools. Problems arise when the authors of these works are not familiar with procedures of licensing, with copyright exceptions (like the quotation right) or collecting societies. Conforming to copyright regulations often implies irresolvable problems for the authors of new art forms. The majority of uses do not fall under the known copyright exceptions so that normally every little sample or snippet has to be licensed and paid for. Needless to mention, most amateur creators (who normally don't earn any money with their work) are simply not able to comply with these requirements. This inadequate balance between copyright protection and the freedom of arts is in my opinion another fundamental shortcoming of today's copyright regulations.

When we talk about authors and creators the multitudes of private home pages by individuals should be mentioned. Especially the enormous group of amateur website authors is widely confused about their obligations arising out of copyright law. What content is protected? What about using pieces of films or music on my website or in user communities? What rules apply to fan art (for example

publishing fan sites that include screenshots of shows or movies or pictures of actors)? These are questions which come up often.

INDICARE: In your view, is today's copyright still well suited for the digital world? Do we need new legislation to cope with the aspects of digital distribution? Or do we simply need better information of consumers and creators of digital content?

T. Kreutzer: As I already mentioned, in my view the relation between copyright protection and copyright exceptions is out of balance today. Copyright regulations neglect the peoples' desire for knowledge, which requires access to copyrighted goods. The fulfilment of this public concern is one of the most imperative tasks in the information society. Looking at the present situation and at the current legislative procedures to me it seems highly doubtful that the national and international lawmakers are serious about proposed objectives like the free flow of information or the universal access to cultural goods and information. There are many indicators for this assessment. To give one example: It is evident that copyright exceptions become more and more restricted while the requirements for the protection are decreased and the rights are expanded. I hardly believe this development is adequate to promote the information society.

In fact I think that the basic approach of copyright needs rethinking. New aspects have to be addressed. In an information society it's not enough to ask how intellectual property can be protected more efficiently. Instead it is imperative to find a way how copyright law can balance all the different interests it affects. In my opinion the attempt to transfer the traditional understanding of copyright to the information society without reconsidering the fundamental ideas has failed. What we need is a new approach that keeps in mind that participation in the information society requires an acknowledgement of strong and coequal users' rights.

More information for consumers and authors is no cure for this unfortunate state of affairs. Providing information and transparency is important in order to increase awareness of the rights and obligations according to applicable law. In other words: to help the affected groups to make the most out of the given situation. But providing information won't help to solve the underlying problems.

INDICARE: Why are independent information portals, like iRights.info, so important?

T. Kreutzer: The particular benefit of iRights.info is that we provide neutral and factual information written in plain and generally understandable language. Most of the information about copyright issues publicly available is either written for experts, based on an uninformed understanding or with a tendentious slant. Especially the campaigns of the entertainment industry seem to operate with selective (often incomplete and sometimes even incorrect) information. I assume that they aim to promote the uncertainty of users and to convey the idea that even the legally permitted forms of usage are prohibited and threatened with severe penalties. To counter such misinformation campaigns is an important task for independent services.

The problem is that establishing such services is quite a time-consuming and expensive affair. Therefore we are very grateful that the German government (the Ministry of Consumer Protection) is financing the iRights project for 18 months.

INDICARE: Mr. Kreutzer, thank you very much for this interview!

Sources

- iRights.info: http://www.irights.info
- Office for Information Law Expertise: http://www.ie-online.de
- Institute for Legal Issues on Free and Open Source Software (ifrOSS): http://www.ifross.de

Status: first posted 24/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=119

Creative humbug

Personal feelings about the Creative Commons licenses

By: Péter Benjamin Tóth, ARTISJUS, Budapest, Hungary

Abstract: For me, there is something fishy about the idea of Creative Commons (CC). The hawkers of this "solution" present the very nature of classical copyright as an *alternative solution*. And they forget to inform the creators about the side effects.

Keywords: opinion – Creative Commons, copyright law

Introduction

The "Creative Commons licenses", a set of standardized general contract terms and conditions, have conquered the world in a short time. We could even say, that "A spectre is haunting the World – the spectre of Commonism". Why could it spread so quickly? What did it offer in comparison with the other similar model licences?

Suggestions – demystified

It mainly offers *suggestions,* in my opinion. The CC organization is really cautious, so the main characteristic of their communications strategy is not written down. The official explanations can be found at the CC website (cf. sources) – but the real image of CC is built up by untold *suggestions.* I would like to present you some of these implied suggestions – demystified.

You could say that it is easy for me to accuse CC on the basis of suggestions. I would rather say: it is very hard to debate with intimations, with a "whispering campaign"; the real intention of CC remains unclear.

1.) "Classical Copyright" vs. "Creative Commons"

CC licences suggest, that the main feature of classical copyright is "*All rights reserved."*, whilst the approach of CC licenses is "*Some rights reserved."*

This juxtaposition is simply false. Copyright provides a list of exclusive rights to the rightholder, from which he decides which ones he wishes to "sell" or grant and which to retain. The "Some rights reserved" concept is therefore not an alternative to, but rather the very nature of classical copyright.

Although in the deeper pages of their website CC acknowledges that their licensing system is based on copyright itself, you just need to write the following words: "*Creative Commons"* and "*alternative"* into Google to find out how many people do not recognize this legally evident acknowledgment, and how many people are rather impressed by their *suggestion*.

2.) "Select a jurisdiction"

The CC likes to stress that their licenses are adapted to many jurisdictions. Let us look at a short quotation from The Register (2004): "*Such legal adaptation work is going on now in around 60 countries"*. Sometimes misunderstandings arise in this context. Let there be no mistake: the CC licenses may be adapted *to* many jurisdictions, but they are not adopted *in* any jurisdictions.

The CC licenses are freely available model contract forms, tailored to the requirements of several jurisdictions. The state is not in a position to adapt or enforce the use of these uniform licences.

3.) "Copyright prevents the free flow of information"

"CC licences are about removing the barriers to sharing information" (Guy and Kelly 2005). This sentence and the whole notion of CC is based on the misbelief that copyright prevents the free flow of information.

This again is a false interpretation of copyright, which will never protect mere facts or information. According to the Berne Convention, Art. 2 (8): "*The protection of this Convention shall not apply to news of the day or to miscellaneous facts having the character of mere items of press information."* The 1967 international diplomatic conference in

Stockholm gave an authentic interpretation of this rule. As we can read in the report of Main Committee I: "*The Convention does not protect (...) miscellaneous facts, because such material does not possess the attributes needed to constitute a work"* (see e.g. Ricketson 2003).

It means that anyone can base his work on the conclusions and facts and all available data of scientific works by other authors. It is only the norms of professional ethics that prescribes that credit should be given to the original researcher. To bring another example: new and exciting musical chords or performing styles can freely be used by other musicians – not because the original artists are generous, just because the scope of copyright does not extend to these elements.

4.) "On the internet you do not need a publisher to reach the public."
Technically this is true. But let us not forget that in the last decades it has always been true regarding the offline world as well. The musicians have had the possibility to prepare their own sound recordings and sell them and to organize their own concerts. The authors have been able to publish their own works. The technical and legal possibility however does not mean that financially these "self-uses" are profitable.

It is not the "*scantiness of goods"* in the offline world that justifies the existence of publishers (professional actors in the selling of content to consumers), rather the "*plenitude of supply"* on the market of contents. If you are not well-known in the public, who will listen to your music or buy your book from a list consisting of 5,000,000 elements in alphabetic order?

5.) "There is no need for this wide copyright protection."
Another implied suggestion of the CC-ideology is that if many authors decide to narrow the exercise of their copyrights, it can be a reason to reduce the strictness of statutory copyright protection. This theoretical conclusion would be totally mistaken.

Even CC-authors need to eat. They need money for existence and creation. When they decide not to exercise some of their copyrights, they do not give up their living for the noble idea of free flow of information – they have some other intent to do so (for example they "advertise" themselves to earn money from personal presentations, or they already have another constant source of income). Therefore their decision should not affect the possibilities of those authors, who need to secure their living from their works.

Hidden facts – unveiled

The other reason for the quick spread of CC licences is that some of their characteristics are concealed, hidden from the public and hidden from the right holders using them. Now I would like to present you two of these circumstances – unveiled.

1.) Commons Deed vs. Legal Code
One of the sources of misunderstanding regarding the nature of CC licenses between the right holders is that there are three forms of a license:

- one that can only be read by a computer (Digital Code)
- one that can "only be read" by a lawyer (Legal Code)
- one that the other part of the world can read (Commons Deed).

The basic version is of course the Legal Code, and this version is "translated" into the other two forms. The problem is that the authors wishing to use the CC license will generally read only the "Commons Deed" version. They will not have the money or possibility to take advice from a lawyer specialized in copyright, and therefore most of them will necessarily lack important information regarding the licence.

The CC webpage suggests, that Commons Deed is nothing else than "*a human-readable summary of the Legal Code (the full license)"*. Unfortunately this is not true; there is lots of information missing in the Commons Deed form. Every such difference implies the danger of misleading the author.

You can read the Commons Deed form, the "Frequently Asked Questions" or "Licenses explained" pages of the CC website (cf. sources), you will not find some of the most important elements of CC licences. You can

only find this information on the bottom of a deep page:

"Every license
– applies worldwide
– lasts for the duration of the work's copy right
– is not revocable"

Has any of you ever noticed it? Is every author using this licence aware of these conditions?

The CC licences last for the whole term of copyright, and binding to the heirs of the authors as well. They are effective worldwide, and you can never change your mind, which is anyway clearly forbidden by a number of copyright acts. It means that a CC license is even more extortionary than an exclusive "buy-out" contract from a global media company, where the author at least gets some money, and according to the legal regulations can revoke the license in some circumstances. To bring another example, a collecting society is obliged to give the possibility to its authors to "take back" their rights if they are not content with the working of the society, and they also have the right to limit the territorial scope of the management of their rights.

In the CC licences the author does not have the right to test, to try out this solution. If he decides – inspired by the insufficient information of the over-simplified descriptions – to use the CC licences, he and his heirs will never be able to change their mind, even if they found out that their decision did not meet their expectations.

Therefore I think that we have to handle with care the statements of CC that their licences do not mean the giving away of copyright. At least it *empties* the essence of copyright.

2.) Unenforceable rights
An edifying excerpt from the Frequently Asked Questions of the CC webpage:

"Will Creative Commons help me enforce my license?

No, we will only provide the license, plus a plain-language summary and machine-readable translation of it. We're not a law firm. We're much like a legal self-help press that offers form documentation – at no cost – for you to use however you see fit. We cannot afford to provide any ancillary services particular to your situation and, in any case, our mission does not include providing such services."

Let me translate it this way: CC provides you legal tools to retain some of your copyrights. But when it comes to the enforcement of these rights, they simply shrug their shoulders. But is it really about not having enough sources to "include providing such services"? Is it not about the fact, that the rights that an author retains when using CC licences are not enforceable in practice?

Let us try to summarize the enforcement problems stemming from the use of CC licences:

a.) "*Non commercial. You let others copy, distribute, display, and perform your work – and derivative works based upon it – but for non commercial purposes only."*

- although the CC website talks about the possibility that a work under the "non commercial licence option" can still earn money from those who are using it for financial gain, in practice this possibility is minimal, almost non-existent. Why should anyone invest in works that are already widely available for free?
- on the other hand: how could an individual author control the uses of his works? In many cases the users are able to hide their financial income, even professional enforcement bodies are facing difficulties in finding them. In case someone uses these works for profit, the authors will not be able to find the users or to achieve a fair royalty rate (because they will not be able to monitor the uses and the incomes of the user). And they will also not be able to trust someone to enforce their rights on a business basis – because there is no business in monitoring usually-free uses.

Although it sounds good for several authors that only non-commercial uses can be carried out freely, in practice the author will not be able to distinguish between commercial and non-commercial uses. Therefore in many

cases the "non commercial licence" practically means that the author puts his works into the public domain.

b.) *Micromanagement*. If we see the most developed part of collective management of copyright (the licensing of musical works), we can see that there is a hundred-year-old equilibrium between the free choice of authors on one hand, and the effective rights management on the other. Although the author has the theoretical right to licence every blond-haired singer to sing one of his songs every second Saturday afternoon for free, this right would not be enforceable.

Therefore the collecting societies created a solution in their field (that is – since the beginning of the 70's – also accepted by the European Court of Justice), in which the decisions of the authors regarding the management of their rights e.g. (i) always refer to a certain period (1 year); (ii) always concern all their works; (iii) are always effective for all uses in a certain mode of use. Of course there may be differences between the societies in the flexibility regarding the choices of the authors, but one thing is common: they do not want unenforceable rights. And although this may seem for the outsiders as a limitation to the free choice of the author, *in reality the value of a less-flexible right may be higher than the unenforceable "nimbleness"*. This statement should also be true for the CC licences.

c.) *Collision of national contract laws*. The contract laws (and in particular copyright contract laws) of national jurisdictions vary across a wide range. The CC licences have their roots in the US law (the "model" is the American one, and every national adaptation has to have the approval of the CC-centre), which differs significantly from continental law systems.

- One of these problems is that a CC licence is not a contract in itself, it is a unilateral statement (contract proposal) by the author. In this case the irrevocability of a statement that licences anyone-anytime-anywhere to use the work free of charge, could mean a renunciation of rights, which is not possible in several jurisdictions.
- In some jurisdictions the CC licence will not meet the requirements of formal validity of contracts.

The licenses with different scope lead to licensing chaos and indemnity confusions.

Bottom line

Creative Commons is a system that alleges that it is more flexible than the classical copyright licensing models. In reality however, where this system is flexible, it creates unenforceable rights. And when it comes to terms of validity or irrevocability of the licence – it turns out to be inflexible.

Sources

- Berne Convention, Art. 2 (8): http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html
- CC website: http://creativecommons.org
- Guy, Marieke and Kelly, Brian (2005): QA Focus information for digital libraries, INDICARE Monitor Vol. 2, No. 2, 29 April 2005; http://www.indicare.org/tiki-print_article.php?articleId=92
- Ricketson. Sam (2003): WIPO Study on limitations and exceptions of copyright and related rights in the digital environment, prepared for the Ninth Session of WIPO Standing Committee on Copyright and Related Rights, 2003 http://www.wipo.int/documents/en/meetings/2003/sccr/doc/sccr_9_7.doc, p.11
- The Register: Germany debuts Creative Commons; http://www.theregister.co.uk/2004/06/15/german_creative_commons/

About the author: Dr. *Péter Benjamin Tóth* is a legal counsel at the Hungarian musical collecting society ARTISJUS. He is also a member of the Hungarian Copyright Expert Group. He can be contacted in e-mail ptoth@artisjus.com

Status: first posted 24/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=118

Licences for open access to scientific publications

A German perspective

By: Ellen Euler, Centre for Applied Legal Studies, Karlsruhe, Germany

Abstract: Scientific research depends on easy and timely access to and use of existing scientific and scholarly research results, which in our times are mostly in digital form. Open Access promises to be a solution to this problem. To realise Open Access it is not enough to archive publications on a server. Rights have to be granted to the general public by applying licenses. The state and role of CCPL, DPPL, SCPL is discussed with respect to scientific publishing and research. What is also required to make Open Access successful is awareness of authors to which this article wants to contribute.

Keywords: legal analysis – Creative Commons, open access, Science Commons, scientific publishing – Germany

Introduction

The scholarly and scientific communication system is a crucial aspect of social benefit as it stands for scientific progress and information. However this system is in a state of severe crisis (cf. Boyd and Herkovic 1999, Parrot 2004, Kuhlen 2004). This information crisis has two contradictory aspects: on the one hand the "information overload" and on the other hand the "information enclosure". Even though the sum of the publications is ever growing due to the ease of producing, publishing and withdrawing information in the digital age, the access to and the use of digital publications is being more and more restricted by the privatization of scholarly and scientific information through copyright and patent law legislation. In Germany for instance the § 53 a UrhG will be cancelled to the end of 2006 (§ 137 k UrhG). Formerly intellectual property rights where the exception, now they are the rule.

Scientific research depends on easy and timely access to and use of existing scientific and scholarly research results that are mostly digital in our age. Open Access promises to be a solution to this problem by using the possibilities of improving the scientific and scholarly communication chain provided by electronic delivery methods. The *science commons* offers a solution for how open access to scientific publications can be gained. But first of all, what does open access mean to scientific publications and what is the role of the *science commons license*?

Open Access

The definition of "open access" is contained in the Budapest, Bethesda, and Berlin public statements. Even though they differ from one another in small ways, they agree on the essentials. The common ground is called the Budapest-Bethesda-Berlin or BBB definition of open access (cf. Suber 2004). Open access to scientific publications means the worldwide, cost free, immediate access to the full text of the publication and the possibility to distribute and use it, and the deposition in at least one online repository using suitable technical standards.

Two models of how Open Access can be realised are proposed by the open access movement (cf. also Poynder 2005 with respect to the golden and the green road):

1. freely available electronic journals, and
2. author self-archiving of research papers on institutional or subject-based repositories

To realise Open Access means, to archive the publication and to grant rights to the general public. But how is it possible to grant the rights mentioned above?

Licenses

There exists a huge variety of open content licenses (cf. ifrOSS). To simplify open access by "standardisation" it would be helpful if the scientific community could agree on the use of a single License. But which one?

Some of them are described briefly in the following.

1. Creative Commons Public License

Without doubt the most popular one is the Creative Commons Public License (cf. Creative Commons 2005a). Creative Commons was founded in 2001 at Stanford University (cf. Creative Commons 2005b). The aim of the released licenses is to build a layer of reasonable, flexible copyright into the increasingly restrictive default rules. The licenses are a tool to reduce barriers to creativity. Initially Creative Commons addressed "Cultural Creatives" (musicians, film-, photo- and image-makers) but not the artists of words. In other words the Creative Commons Public License was created for artists and not authors. But with its different modules authors can also express which rights they want to retain and so the licenses are also used for publications. In this context the specification "Attribution-no Commercial-no Derivatives" (cf. Creative Commons 2005c) is used most often. This confirms the results of the RoMEO study (cf. RoMEO Project) "How academics wish to protect their OA-research papers". The license was adopted in many countries; in Germany it has been available since June 2004 (cf. Dreier 2004).

2. Digital Peer Publishing License

In October 2003 the German Ministry of Science and Research of North-Rhine-Westphalia acted as initiator for the Open Access Initiative "Digital Peer Publishing NRW" which created the Digital Peer Publishing License (cf. DiPP), which was intended to encourage the foundation and expansion of scientific eJournals when the Creative Public License was not yet available. Up to now there exist 10 e-journals using the license. The DPPL was initially created for the authors of scientific publications with the goal of increasing the number of high-quality scientific publications as well as developing and establishing new methods of network-based cooperative information management, which will in turn enable high-speed, open, and transparent digital peer publishing in an appealing environment. In practice it doesn't differ very much from the CCPL. The only significant differences are in the specifications of retained rights but not in the application fields.

Table 1: Comparison of CCPL and DPPL

	CCPL	DPPL
Differences	- Designed for creative content; - 3 layer system; - modular building block system; - does not distinguish by carrier medium	- Designed for scientific content; - three different licences; - distinguishes between electronic and analogue carriers
Obligations	- Reference to license; - no digital rights management (DRM) - no copyleft; - credit to the author	- Reference to license; - retention of open access and credit to the author; - history
Advantages	- internationally networked; - building block system; - machine-readable metadata	- Proximity to science; - regional partners; - changes can be restricted in scientifically specific manner
Disadvantages	- Completely or not at all alterable; - use cannot be restricted	- Low degree of international linkage

Science Commons

Its specific application to the needs of the scientific communication distinguishes the Science Commons Project from the Creative Commons Project. Science Commons (cf. Science Commons 2005a) is an exploratory project to apply the philosophies and activities of Creative Commons in the realm of science. As an accomplishment of the Creative Commons Project it looks at the legal frictions that hinder reuse of scientific discoveries and might lead to discouraging innovation. The project focuses on patent rights and solutions to the increasing enclosure of in former times non protectable "raw facts" (for more information see Science Commons 2005b). The goal is to achieve the creation of a larger "Science Commons" built from private agreements, and technical standardization. The "some rights reserved" approach is adopted from Creative Commons, the parent organization. It is intended to support open access to scholarly research in a wide range of disciplines. Science Commons works in three project areas: Publishing, licensing, and data. This article focuses on publishing.

The process of scientific publication includes other applications of licences such as:

- Licenses to other publishers or journals;
- Licenses on Pre/postprints;
- Licenses for author self-archiving;
- Mechanisms for author self-archiving;
- Legal implications of Open Access business models;
- Application of machine-readable licenses to documents.

Here in addition to the Creative Commons licenses, the SCPL is generated. But as mentioned above, the Project started in early 2005 and is still at the beginning. Up to now drafts for licences don't exist and groups therefore are being encouraged to use the Creative Commons standard licenses for the time being. The initial focus is more on technical approaches which make self-archiving easier, and on an education and outreach campaign so that both institutions and authors understand the importance of the issue. So far it is unclear at what date the SCPL will be available in the US, or when or if it will be adopted (like the CCPL) in European countries.

A brand new part of the Science Commons publishing project is the Open Access Law Program, that supports "Open Access" to legal scholarship (for details see: http://sciencecommons.org/literature/oalaw). The Open Access Law Program (OAL Program) consists of a set of resources to promote open access in legal publishing. These resources include:

- Open Access Law Journal Principles;
- Open Access Law Author Pledge;
- Open Access Model Publishing Agreement.

Unless the SCPL is available in Germany authors can (and should) use the Creative Commons Public License as well as the Digital Peer Publishing License (or both as they do not exclude each other) to grant rights and enable Open Access.

1. Practise of granting rights

The practice of granting rights with a Creative Commons License is very easy. To generate the License only two questions have to be answered (Allow commercial use? Allow Alteration?). The license gets generated in a HTML-Code, which can be simply inserted by copy and paste. The website of Creative Commons also provides a software application, the so called "CC Publisher" (cf. Creative Commons 2005c). It provides free hosting as well through the Internet Archive. The Science Commons Project is going to extend this tool to have it more scientifically driven, as the current interface was designed for cultural creators. Such a software doesn`t exist for the Corresponding DPPL. The license has to be inserted manual, which may hinder the broad use.

2. Author`s Addendum

But the technical problems are only one thing that has to be solved. Currently another big problem is the legal impossibility of granting rights imposed by the contract with the publisher. While some journal publishers already utilize author-friendly agreements, others do not. They still insist on transfer of all exclusive rights from the author, the so called

"buy-out contracts", no matter whether there really is an intention of actually using these rights later on. Fortunately, many publishers will agree to changes in their standard agreement. The uncertainty of what and how to change such author agreements and mark up the publisher's standard agreements could be solved by the "Author's addendum" proposed by SPARC (SPARC 2005). It is a simple form that amends the "Publisher Agreement" and is attached to it. By using the SPARC Author's Addendum the author retains his right to make his article available in a non-commercial open digital archive on the Web. Up to now there exists only an English draft of this form, but SPARC Europe is about to publish the German version (ask bargheer@mail.sub.uni-goettingen.de for detailed information).

Bottom line

Currently Open Access to scientific publications is achieved by archiving the publication and granting rights. To grant rights means to license the publication with an Open Content License. In most cases the Creative Commons Public License is used as it provides a good fit for academic research papers. In addition in Germany the Digital Peer Publishing License is used. The Science Commons License is not going to be an amendment of the Creative Commons License for scientific publications, but focuses on other areas of licenses. Up to now it is yet unclear, when the licence is going to be available in the USA, or when or if it will be adopted in Germany. In the meantime the existing licenses should be (and are) used also for scientific publications. To enable the use of open content licenses by authors, the publisher agreements have to be amended. This can be realised by a standardised addendum as proposed by SPARC. But as it is within the capacity of the individual author to make his or her work openly accessible, the most important thing remains to inform the author. It is speculated that most of the authors do not make their work openly accessible because they are not informed. We need more education and outreach campaigns, so that both institutions and authors understand the importance of the issue.

Sources

- Boyd, Stephen and Herkovic, Andrew (1999): Crisis in scholarly publishing: Executive summary; http://www.stanford.edu/~boyd/schol_pub_crisis.html;
- Creative Commons (2005a): www.creativecommons.org
- Creative Commons (2005b): http://creativecommons.org/about/history
- Creative Commons (2005c): http://creativecommons.org/licenses/by-nc-nd/2.0/de/
- Creative Commons (2005d): http://creativecommons.org/tools/ccpublisher
- DiPP (Digital Peer Publishing): Licenses at http://www.dipp.nrw.de/lizenzen/index_html?set_language=en&cl=en
- Dreier, Thomas: Creative Commons in between unlimited copyright and copyright anarchy. INDICARE-Interview by Bettina Krings. INDICARE Monitor, Vol.1 No 4, September 2004; http://www.indicare.org/tiki-read_article.php?articleId=40
- ifrOSS (Institut für Rechtsfragen der Freien und Open Source Software): http://www.ifross.de/ifross_html/opencontent.html
- Kuhlen, Rainer (2004): Wie öffentlich soll Wissen für Wissenschaft und Unterricht sein? Anmerkungen zum Urheberrecht in der Informationsgesellschaft; http://www.inf-wiss.uni-konstanz.de/People/RK/Publikationen2004/rk_urh_in_D-fuer_ie-buch.pdf
- Parrott, Jim: The crisis in scholarly publishing (2004): Scholarly Societies Project http://www.scholarly-societies.org/crisis.html;
- Poynder, Richard**:** The role of digital rights management in Open Access. INDICARE Monitor, Vol. 2, No 2, April 2005; http://www.indicare.org/tiki-read_article.php?articleId=93
- RoMEO Project: http://www.lboro.ac.uk/departments/ls/disresearch/romeo/
- Science Commons (2005a): www.sciencecommons.org
- Science Commons (2005a): http://science.creativecommons.org/about/scbackground
- SPARC (2005): Author's Addendum: http://www.arl.org/sparc/author/addendum.html
- Suber, Peter (2004): Praising progress, preserving precision. SPARC Open Access Newsletter, issue #77, September 2, 2004 http://www.earlham.edu/~peters/fos/newsletter/09-02-04.htm

About the author: *Ellen Euler* LL.M., researcher at the Centre for Applied Legal Studies (Zentrum für Angewandte Rechtswissenschaft), University of Karlsruhe. Currently she is leading a project about Creative Commons. Contact: euler@ira.uka.de

Status: first posted 24/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=117

Norwegian implementation of the EUCD Article 6

By: Thomas Rieber-Mohn, Faculty of Law, University of Oslo, Norway

Abstract: On 11 February this year the Norwegian Ministry of Culture and Church Affairs submitted its long awaited White Paper (2005) on amendments to the Norwegian Copyright Act (1962). The purpose of the proposed amendments is to bring Norwegian copyright law into consistence with the European Copyright Directive (EUCD 2001). The approach chosen as to the implementation of EUCD Article 6 contains some rather innovative elements and goes far in protecting consumers' interests – perhaps too far compared to the EUCD.

Keywords: legal analysis – copyright law, EUCD, technical protection measures – Norway

The protection scheme

As required by EUCD Article 6, the White Paper proposes a twofold protection scheme for technological protection measures used by right holders to protect their works (and other subject matter): partly, it prohibits (the act of) circumvention of such measures; partly, it bans certain preparatory acts of trafficking in circumvention devices. (Additionally, the proposal contains a provision protecting rights management information, cf. EUCD Article 7, but this provision will not be treated here).

Protected measures

The proposal does not include any statutory definition of "technological measures". However, it is made clear that anti-circumvention protection only applies to measures that are used in order to control either the *making of copies* or the *making available to the public* of a protected work. This delimitation of protected measures is not coincidental: The said acts coincide with those defining the copyright holder's exclusive rights under Norwegian copyright law; hence they are referred to in the preparatory report as "copyright relevant acts". The delimitation of the anti-circumvention protection to measures that control "copyright relevant acts" reflects one of the Ministry's overall intentions, namely to tie the protection as close as possible to the contours of the copyright monopoly, without disrespecting the EUCD-requirements.

EUCD Article 6.3 defines "technological measures" as measures that in the normal course of their operation, are designed to prevent or restrict acts "not authorized by the rightsholder". From this express reference to an authorization, the Norwegian Ministry deducts that Article 6.3 only encompasses measures controlling acts covered by the *copyright* monopoly (!). Arguably, this is not a "waterproof" deduction, but the reasoning (of the Ministry) is as follows: For the right holder to be in a position to *authorize* certain uses, such uses must somehow have been made subject to her supremacy. Relevant in this relation is (in the Ministry's view) only the monopoly granted to her *qua copyright holder*. Thus, (again in the view of the Ministry) protection is required by the EUCD only where measures are used to regulate conduct that falls *within the ambits of the statutory monopolized acts*.

This means that a measure that regulates conduct outside the ambits of the statutory monopolized acts (e.g. performance of a work within the private sphere), cannot *itself* constitute the basis for anti-circumvention protection. It also means that "copyright relevance", in the sense just described, can-

not be gained through monopolizing an act by contract.

It should be pointed out that, whereas the said definition of "copyright relevant acts" implies a demarcation towards acts that neither can be classified as *copy making* nor *making available to the public*, it does *not* exclude acts that fit such a classification, but nevertheless positively have been *lifted out of* the copyright monopoly (through copyright exceptions). If, for instance, a measure merely controls private copying – a conduct exempted from the Norwegian copyright monopoly through a statutory exception – it will still fall within the sphere of protected measures, since the conduct as such (copy making) falls within the ambit of one of the monopolized acts (copy making). This is slightly different when it comes to the exclusive right to make available to the public, since there, the monopolized act *itself* is delimited to the public sphere.

One very important modification has to be made to the just described point of departure: Technological measures applied in order to protect "copyright relevant acts", but which *also* control conduct outside the statutory monopolized acts (e.g. private performance), shall still be protected. In other words, the *additional* feature of usage rules controlling non-"copyright relevant" acts shall not disqualify the measure as such from protection (as long as it *also* is aimed at controlling a "copyright relevant" act). If, for instance, a copy control mechanism at the same time blocks playback of a work within the private sphere, it will still – in principle – be within the sphere of protected measures. However, as we shall see just below, a special exemption is introduced as to enable private enjoyment.

Right to circumvent to enjoy within private sphere on 'relevant playback equipment'

Even though such "combined" measures fall within the sphere of protected measures, one important – and, compared to the text of the EUCD, rather innovative – modification is made as to the *scope of protection* in this regard: If a "combined" measure hinders what is called "enjoyment within the private sphere" of a copy of a work, the consumer may circumvent the measure in order to "enjoy" the work on what is called "relevant playback equipment". The preparatory report accentuates, that this is not a delimitation of the sphere of protected measures, but rather a limited exception *to the ban* of circumvention: Even though the measure as such is protected, the consumer may lawfully circumvent in order to pursuit this specific purpose.

Of course, the provision raises the question of which equipment shall be deemed as "relevant". According to the initial preparatory report, the relevance is relative to the format in which the work has been lawfully acquired. In the end, according to the initial preparatory report, one must ask which expectations as to playback equipment the consumer reasonably may have with respect to a given type of product. Using a musical work as example, the initial preparatory report stated that circumvention of a technological measure applied on a musical CD would be lawful if needed in order to play the CD on a CD player, but *not* if the purpose was a conversion into MP3. In other words MP3 players were not to be considered "relevant playback equipment" as to the musical files on a CD. As a curiosity; this last exemplification in the initial preparatory report (of an exception to an exception) has resulted in the proposal being named "the MP3 Act" in the Norwegian public debate.

While writing this article, the first division hearing in the Parliament has passed with a majority voting against the Ministry's proposal to exclude MP3-players as relevant playback equipment for music files on a CD. Thus, as it looks at the moment, circumvention will be lawful if necessary in order to convert the music files on a CD into MP3 (or similar formats).

The scope of the said "right to circumvent" is narrowed down considerably by an additional clarification made in the preparatory report: If a digital file is made available *on-demand through a digital network* and the parties in this connection agree as to which media-player can be used to experience the file, that contractual regulation shall deter-

mine what shall be deemed "relevant playback equipment". In other words, when it comes to such services, the "relevance" of playback equipment shall be subject to contractual *freedom*. After this, the said "right to circumvent" is, in practice, reduced to situations where the copy of the work is distributed on a physical carrier (e.g. a CD or DVD) or online-but-not-on-demand. Statements during the Parliament hearing indicate that the scope of the exception might be further narrowed down to comprise conversion from CD to MP3 *only*.

The said "right to circumvent" in order to enable private playback within the private sphere must also be seen in relation to another amendment proposed in the White Paper: The existing freedom of users, under Norwegian law, to make copies of works for private use purposes, is upheld. However, it is made subject to one additional qualification: Private-use-copying shall be allowed only where based on a so-called "lawful source of copying". This means that the copy or transmission, upon which the reproduction is based, must be lawful; it must have been produced or made available in accordance with a permission by law or by the right holder(s) concerned. In the absence of such authorisation, for instance if a work has been illegally uploaded to the Internet or made available through a p2p-network, the source will not be lawful and may hence not serve as the basis for (lawful) private-use-copying. It is made clear in the White Paper, that if any copies should be made in connection with, or as a result of, the performance of the said "right to circumvent", such copies shall *not* be regarded a "lawful source of copying". Thus no further copies may (lawfully) be made on such a basis.

"Interface" towards copyright exceptions

As required by EUCD Article 6.4, the White Paper also contains an express "interface" towards certain copyright exceptions. The copyright exceptions covered regard certain uses related to teaching, recording for use by health institutions, retirement homes, prisons etc., libraries, museums and archives, disabled persons, ephemeral recordings and public negotiations, document inspection, interrogation and evidence. The option of creating an "interface" for the private copying exception has so far not been used. In accordance with Article 6.4 fourth paragraph, the "interface" shall not apply where a protected work is being made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them (the so-called on demand services).

The proposed "interface" places an *obligation* upon right holders to respect the concerned copyright exceptions while designing their technological measures. However, the question of *how* right holders shall enable required uses can be regulated through contracts between the parties. If the right holder does not voluntarily enable the use required by the relevant exceptions, Sect. 53b second paragraph provides the following failsafe mechanism, which can be triggered by the beneficiary (unofficial translation):

> "If the right holder, after a request from a beneficiary under the above-mentioned provisions, does not grant such access as mentioned in the first paragraph, he may, upon the beneficiary's request, be ordered to provide the information or other assistance needed to obtain utilization of the work in accordance with the purpose. Requests shall be presented to a committee appointed by the Ministry according to procedures established by the Government. The committee may, in addition to such order as mentioned, decide that a beneficiary under the mentioned provisions unhindered of Sec. 53a [the proposed ban of circumvention] shall be allowed to circumvent applied technological measures if the right holder fails to comply with the order within the time limit decided by the committee."

Indeed, this provision empowers the beneficiary with an effective means to enforce her copyright exception privileges – even against the will of the right holder. The beneficiary may well negotiate with the right holder about these matters, but she can always fall back on claiming the copyright law solution

to be enforced. Upon her request, such enforcement will be carried out. This is done primarily by obliging the right holder to provide, within a defined time limit, the information or other means needed in order to use the work as defined in the relevant copyright exception. Subsidiary, this is done by permitting the consumer to circumvent the measure if the right holder fails to do so. Thus, ultimately, the Norwegian "interface" grants a *right to circumvent*. And – perhaps even more importantly – it lies with the consumer to trigger this right.

Bottom line

The proposed Norwegian implementation of EUCD Article 6 links the definition of protected measures directly to the acts monopolised by copyright law: as the point of departure, only measures that are used for the purpose of controlling so-called "copyright relevant acts" are protected. Further, the ban shall not apply to acts of circumvention that are needed in order to enjoy the work within the private sphere on so-called "relevant playback equipment". The proposed "interface" obliges right holders to respect the relevant copyright exceptions while shaping their technological measures. If they do not do so, the beneficiary can file a complaint to a specialist tribunal empowered with the authority to – ultimately – grant a permission to circumvent.

Arguably, the Norwegian Ministry has all in all adopted a balanced – though perhaps controversial – interpretation of Article 6. Whereas the EUCD itself, by some, would be described as rather "toothless" when it comes to offering *real* protection to the consumer-side, the Norwegian proposal certainly puts power behind the good intentions in this regard.

Sources

- EUCD (2001): Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf
- The Norwegian Copyright Act of 12 May 1962 no 2 (unofficial English translation), available on: http://www.unesco.org/culture/copy/copyright/norway/fr_sommaire.html
- The White Paper (official Norwegian version), available on: http://www.odin.dep.no/filarkiv/237235/OTP0405046-TS.pdf

About the author: *Thomas Rieber-Mohn* has prior experience as an IPR-lawyer in Norway and is currently a doctoral research fellow at the Faculty of Law, University of Oslo, where he is working on a PhD project on copyright, DRM and anti-circumvention laws. Contact: Thomas.rieber-mohn@jus.uio.no

Status: first posted 10/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=111

Contractual balance in digital content services

By: Timo Ruikka, Nokia Corporation, Espoo, Finland

Abstract: Alongside copyright balance, the question of contractual balance will gain in relevance as consumption and contract practices change with the evolution of new services. Using the analytical distinction of "consumption use" and "copyright use" the paradigm shift is demonstrated between the "legacy model" of book/CD purchase and new services like iTunes music store and 48-hour online "video rental" services. Admittedly the new focus on contracts goes together with new challenges.

Keywords: economic analysis – business models, consumer expectations, digital contracts, copyright law

Introduction

Digital content services delivered over electronic networks are changing contract practices in how works are offered to consumers. Not everyone agrees with me when I claim that we have seen only early experiments for digital content services and that many other and substantially different bargains will be offered to consumers. But for the sake of argument, let's assume that this is so and consider where this view forward takes us.

The detailed characteristics of new services are enabled by technical protection measures such as Digital Rights Management (DRM). My aim in this article is to illustrate that technical protection measures serve a dual purpose – they are not only used to structure copyright-related aspects of what is offered to the consumer. They are also to a significant extent used to structure the commercial offering, what is the bargain offered to the consumer. My suggestion is that this duality of purpose is relevant for analysis of "fairness" and "balance" of a given offering and that the perspective of contractual balance is an important factor in that analysis.

As this article focuses on the contract aspects, I largely omit discussion of balance under copyright law. Copyright balance involves the system of "copyright rights" and the exceptions and limitations to those rights defining the respective legal positions of the rightsholder and the consumer/user. Important public policy objectives are also served by the existing copyright balance system. These considerations continue to be important, but alongside copyright balance, the question of contractual balance will gain in relevance as consumption and contract practices change with the evolution of new services.

Consumption use and copyright use: technical, legal and commercial duality

When the content of a copyrighted work is accessed in a digital device (computer, TV set top box, game console, mobile phone), and if technical protection measures are not imposed, it is technically easy and convenient to carry out both

- **"consumption uses"**: rendering and playback acts of accessing the work such as listening, viewing and reading; and
- **"copyright uses"**: exploitation acts such as generation of further instances of the work (copies) and distribution, display, performance or the making available of the work to others.

I have here adopted the term "consumption uses" to distinguish consumption opportunities from the special meaning that the noun "use" has in copyright law. Vastly simplified, "copyright uses" are acts within the "copyright rights" of the rightsholder. They do not include what most people associate with consumption, the enjoyment of a work by a consumer.

Technical protection measures are the technical way of addressing risks and opportunities inherent in the multiplicity of uses enabled by the unprotected digital format. Yet it is more or less impossible to "cleanly" address only one of these two sets of uses and not the other. This is due to an overlap of

the legal and technical ramifications of the choices in what is enabled in a service: The more the consumer's "copyright uses" are restricted to preserve the rightsholder interests, the more is the consumption opportunity also affected. The broader the enabled consumption opportunities are, the greater is the risk of unauthorized "copyright uses". But the overlap is not limited to this technical/legal dichotomy. Whether a broader or narrower scope of consumption is offered also is a matter of commercial choice for the distributor and a matter of alternative offerings for the user. From the consumer's perspective, a narrower consumption scope can be quite attractive if it is associated with a substantially different price point. In this manner, use of technical protection measures has technical, legal and commercial dimensions. They enable and are being used for both:

- the structuring of "copyright uses" afforded to the user in a manner that may not conform to the established contours of the balance under existing copyright law; and
- the structuring of "consumption uses" afforded to the user in a variety of ways that may significantly alter the contractual essence of what the user is provided.

Despite some limitations in their design (e.g. creation of derivative works often cannot be supported), DRM solutions – and the "rights expression languages" underlying those solutions – are capable of a very granular articulation of what "consumption use" and what "copyright use" is afforded to a user. From a contract lawyer's perspective, such use of DRM is very likely to alter the contract, the bargain in comparison to traditional models, at least when requirements related to contract formation are met, such as description/disclosure, transparency of terms, reasonable expectations etc. Structuring of digital content services in this manner challenges traditional notions of balance under copyright law – and previous contractual models.

The paradigm shift: old paradigm described

We all are inherently familiar with the printed book and the CD recording. I consider these to represent the "legacy paradigm" of the offline/analog era. I include the (admittedly digital) unprotected CD format here as it is offered to users in exactly the same manner as the analog book. At least the following contractual characteristics typically are present:

- User purchases a permanent copy of the work; no contractual restriction is imposed on the time during which it may be consumed;
- Purchaser acquires legal title, ownership of the physical object – with the property rights in the physical copy (right to undisturbed possession, right to dispose by resale, gift, inheritance etc.);
- No restriction is imposed on the user regarding the number of times the content is accessed, by whom or where this occurs;
- No restriction is imposed regarding type or number of devices for playback/rendering;
- The contract includes neither a license to the user under "copyright rights" nor any curtailment of activities permitted under "copyright exceptions".

Outside the contract, the user is authorized to carry out certain copyright-relevant acts – e.g. legal ability to create copies for non-commercial use or to privately display and perform the work. These authorizations flow from copyright law, under exceptions and limitations to copyright "rights". They have contractual relevance – one hardly can claim they are entirely ignored by the contracting parties. But they are usually not a core part of the contract. The seller does not, as a rule, even have legal license to grant (sub)licenses to consumers and subsequent users under the rightsholder's copyright rights. The traditional book/CD paradigm contractually is a sale of movable property with no express elements of a copyright license. Copyright law fills in the "copyright uses" aspects.

Consumer-oriented discussion about digital works with technical protection measures often compares new services with this "legacy model" of book/CD purchase – mostly unfavourably. To push the point, when one

takes the unprotected CD as a benchmark, practically all restrictions present in the protected digital version tend to be a step backward from the consumer's point of view. Close review of the consumption scope granted, copyright uses enabled and the price point associated with the modified digital service offering may however suggest that a direct comparison to the book/CD paradigm is flawed.

Further, traditional consumption model examples structured as a service – rather than a sale of physical goods – suggest that it is not always offensive to structure both "copyright uses" and "consumption uses" by contract in a manner departing from the book/CD paradigm. Many services impose contractual restrictions that arguably extend to acts the user could engage in without violating copyright. Live performances, movies, museums, galleries etc. prohibit audio taping, videotaping, still photography, creation of painted replicas etc. (In what I regard to potentially mark an act of legislative overkill, videotaping of movie performances was recently (2005) made expressly illegal in the United States under the Family Entertainment and Copyright Act, Public Law no. 109-9).

The iTunes offering

Apple's iTunes service is the technically protected digital content service that at the time of writing this article (June 2005) is receiving the most attention worldwide. The iTunes music store provides protected audio content for use on computers and Apple's portable iPod devices. Based on a review of promotional language at the iTunes website and the U.S. version of the iTunes Music Store Terms of Service (found at http://www.apple.com/support/itunes/legal/terms.html), the commercial proposition on offer can be identified, albeit with some difficulty – even the generally user-friendly Apple site leaves much to be desired in this regard. The following is a decidedly incomplete list of important contractual characteristics, resting on heavy interpretation of Apple's license terms and promotional language:

- User purchases a "permanent" music item (and associated artwork) called a "Product";
- The Product may be stored and used on up to 5 computers and portable devices at any one time, and only on Apple-authorized devices such as Apple's own iPods;
- One iPod can accept and use Products from a maximum of 5 iTunes accounts at a time;
- There is an express limitation of the permitted "use" for personal and noncommercial purposes but the legal nature of possible "uses" does not appear to be defined
- There is no express copyright license to do so – and an express disclaimer of any license granted under copyright – but the user is provided a fairly liberal ability to convert ("export" or "burn") Products into other formats. Of particular relevance is the ability to burn music onto CD disks with relatively few limitations.

The bargain is in some respects materially different from the book/CD paradigm. For instance, the limitation on "use" on Apple-authorized devices only is a significant departure from the book/CD paradigm. But so is the express authority to use the Product on up to 5 devices at the same time – and the possibility to use Products from 5 different accounts (e.g. within a circle of friends or a family) on any one device. While there is no crystal clear copyright license language granting the right to create up to 5 reproductions of each Product to accomplish this, the disclaimer of most other copyright licenses clearly does not extend to this ability to put the music on up to 5 devices. At least to this writer, it seems that there, then, is a contract expressly permitting 5 copies and not objecting to practically unlimited, but unlicensed, burns to CDs (as an aside, I note here that this express authority appears to have relevance to the issue of copyright levies on devices, as the up to 5 reproductions in this example appear to be affirmatively licensed and do not rely on copyright exceptions). Clearly, the bargain is different from the CD bargain for the same content.

The relative success of iTunes at this time is the result of multiple factors – not the least of which is the exterior design and ease of use of the iPod device. There reportedly also are complaints from disappointed users. Nonetheless, the sustained growth and rave reviews of the iTunes/iPod experience seem to suggest that there also are users who, at least so far, are satisfied with what they have received in terms of the "consumption uses" and "copyright uses" enabled by the technical protection measures in the iTunes Products delivered to them.

Network based rental or library loan

A second service example – hypothetical for the purposes of this article, as I have not researched whether such a service already exists – would be a 48-hour online "video rental" service, which could be technically enabled to include:

- Download of a copy of a movie;
- Unlimited number of playbacks within a 48-hour time window;
- Possibly restricted to one device at a time, or to a technically defined location;
- Without technical ability to create permanent copies for future playback.

My reason for raising the rental example here is that, due to its similarity with DVD rentals, it is likely to be recognized by most consumers. If priced at a sufficient differential to the "permanently owned" copy of a work (like DVDs are priced at € 1 or € 2 per rental, in contrast to € 15 for an "owned" copy), it is possible to argue that the bargain, also for the consumer, can contractually be an adequately balanced one – even when ability to create a personal permanently usable copy is excluded. Another service example with significant restrictions closely resembling restrictive terms of analog services is a DRM-enabled eBook library loan – see e.g. at http://ebooks.nypl.org.a description of the New York City public library's eBook service

New focus on contracts – and new challenges

Technical protection measures enable an unprecedented flexibility for distributors of digital protected works to adhere to or depart from existing consumption and contractual paradigm(s) regarding both "copyright uses" and "consumption uses". The restrictions on either use, imposed by technical protection, are not necessarily offensive. What matters is: what is "the deal" and how it is understood. One trend of the shift taking place is a movement away from a product/sale paradigm towards a service paradigm that can be flexibly structured.

This new flexibility is not unproblematic – my objective is not to offer an apology for overly restrictive services. It is easy to get a service offering "wrong": With novel use of technical protection measures, especially with poor disclosure and poor marketing, user disappointment and rejection is often the result. Second, unlimited versatility means that it is difficult and frustrating for users to identify what consumption (and copyright) uses exactly they are getting when they obtain content from multiple services, all having different detailed structures for broadly similar offerings. In this issue of the INDICARE Monitor Philipp Bohn (2005) ably describes typical varieties of subscription services. While variety is welcome in early experimentation, it is not conducive to achievement of more mature success in a mass market. Mass market cannot happen without broad consumer acceptance.

Many consumer, business and public policy challenges need to be addressed. To illustrate the tip of the iceberg in this regard, I here suggest some obvious areas for development:

- How to harmonize multiple offerings serving more or less similar consumer needs, to reduce confusion and match expectation with experience?
- How to improve transparency of terms and remove ambiguity of what is on offer and at what price?
- Should there be some collaborative process to foster "best practices", even coupled with a trust mark to guide consumers?
- What is the role of standard contracts and how should they be generated?

- What effective and proportionate consumer protection tools can be used to address abuses?
- What kinds of support services are needed to address ancillary consumer needs such as restoration of content on broken (or stolen) devices, availability of extensions to time limited works, migration of paid for content between service providers?
- How to best preserve public policy objectives that may be affected by new contract models utilizing technical protection – such as information access and library service – as well as how to ensure access for civil, administrative and judicial purposes (heirs, regulatory, tax, law enforcement, courts etc.) to information within technically protected works?

Bottom line

These are major challenges. Yet I believe the new services can and eventually will provide significant value to consumers, once the experimentation dust settles. New opportunities – lending, rental, even "disposable" consumption of works that one may be quite willing to purchase several times, if priced accordingly – are still largely unexploited.

Sources

- Bohn, Philipp (2005): Rent-A-Star: Do you subscribe to digital music? INDICARE Monitor, Vol. 2 , No 4, June 2005; http://www.indicare.org/tiki-read_article.php?articleId=112
- Helberger, Natali (2005): A2K: Access to Knowledge – Make it happen. INDICARE Monitor, Vol. 2 , No 3, May 2005; http://www.indicare.org/tiki-read_article.php?articleId=102
- Mulligan, Deirdre K.; Han, John; Burstein, Aaron J. (2003): How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use". In: Proceedings of the 2003 ACM workshop on Digital rights management Washington, DC, USA Pages: 77 - 89
- Schaub, Martien (2005): Consumer protection law: setting a standard for the use of digital content. Paper given at the 3rd INDICARE Workshop "Fair DRM Use", Amsterdam, 28.5.2005

About the author: *Timo Ruikka* is Vice President, Industry Initiatives at Nokia's technology Platforms unit. Contact: timo.ruikka@nokia.com

Status: first posted 21/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=113

Rent-A-Star: Do you subscribe to digital music?

By Philipp Bohn, Berlecon Research, Berlin, Germany

Abstract: Apple's iTunes Music Store (iTMS) has long been regarded as the undefeated champion of legal music downloads. Recently, companies like Yahoo!, RealNetworks or Napster have peppered the competition offering music on a subscription basis. This article wants to give you the basic facts this business is built on. It takes a look at the different business models and the Digital Rights Management systems involved. The advantages and inconveniences are weighed from the consumers', online retailers' and the music industry's perspective.

Keywords: economic analysis – business models, consumer expectations, music markets, stakeholders, subscription services

Placing the bets

Basically, there are two business models when it comes to selling music online: pay-per-download (à la carte) or subscriptions. Consumers are used to owning a CD and disposing of its content in any way. They "have been buying music for 50 years. They want to replicate that experience online", says *Eddy Cue*, Apple's vice president of applications and Internet services, overseeing its benchmark iTMS (Hansell 2004). But

some people think different: "We see subscription becoming the predominant contribution to our business very soon", *Chris Gorog*, Napster's CEO (Banerjee and Garrity 2004).

iTMS and most other online music stores today bill customers by the track or album they choose to download. In contrast, companies like Napster, Yahoo! and RealNetworks offer a monthly flat fee in exchange for unlimited downloads.

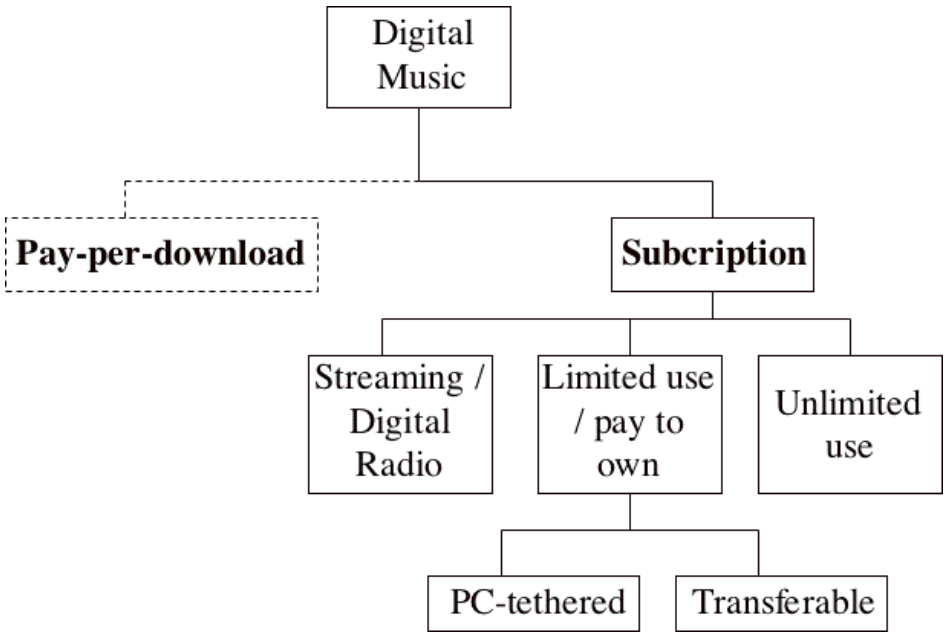


Figure 1: Online music business models

Figure 1 summarizes the various concepts of music subscription services ("Pay-per-download" is mentioned for the sake of completeness and contrast. The figure is not supposed to suggest homogeneity within that field). Streaming subscriptions or digital radio have already been introduced to the market for some time. This article focuses on the second environment: subscription. In that environment, you can listen to and download as much as you want as long as you pay the fee. Some services allow consumers to listen to the music on their PCs only (PC-tethered), while others make files transferable to portable devices. The third scenario is covered by smaller companies like Wippit from the UK, which will not be covered by this article.

Basics of usage rights management in subscription services

While subscription models provide unlimited access to music, the DRM regime is much stricter. The main difference between actually buying songs and merely renting them is the expiry of files upon cancellation of the subscription. Once you stop paying the monthly or annual fee, the files that you have downloaded cannot be played anymore. If you want to listen to them again, you must prolong the contract and the files are unlocked. In case files are made transferable to portable devices such as an MP3 player, licenses are programmed to expire on a set date. Subscribers need to connect their mobile devices to their PC platform in order to update usage rights on a regular basis.

The prerequisite for transferring protected music to portable devices to-date is Microsoft's Windows Media Digital Rights Management for Portable Devices (WMDRM-PD, "Janus"). Its real-time clock checks if a subscription license is still valid. If so, the file can be played-back until the end-date of the license. A license contains terms and conditions, or usage rights, by which content usage is regulated (Guth 2003).

In case the consumer has decided to own a track that does not expire, subscription providers offer him or her to buy it for a fee on top of the subscription price. The track can then be played as long as the consumer wishes and be burned to a CD a definite number of times.

The business models

This article takes a look at business models that are trying to challenge iTunes' business model, namely RealNetworks' Rhapsody, Napster's To Go service and the recently launched Yahoo! Music Unlimited.

RealNetwork's Rhapsody: Real offers four different retail schemes. The low-end offer allows consumers to listen to 25 songs per month for free and eventually buy one or more for the usual 99 cents. Upgrading to US $ 4.99 per month gives access to web radio with a limited option to personalize. Actual subscription starts at US $ 8.99, allowing listening to an unlimited number of tracks on your home computer. In case consumers want to transfer the tracks to a mobile device, the monthly fee is raised to US $ 14.99. These tracks cannot be kept and burned – owning costs 89 cents per song. Unlike other services, tracks are compatible with Apple's iPod, which is popular with allegedly 70 % of consumers (Seff 2005). This issue is highly debatable, as Real's policy is in disaccord with Apple. Availability to date: United States only.

Napster: As a basic service, the monthly subscription fee is US $ 9.95, while you have to pay 99 cents for a permanent copy. In case you subscribe to Napster To Go, this fee rises to US $ 14.95. In return, customers can transfer their files to a portable device. The company was the first to employ Microsoft's Janus DRM system that is necessary if files are to be transferred to external devices. Availability to date: United States, Canada, United Kingdom.

Yahoo! Music Unlimited: There has been quite a buzz about this service, mainly because of its pricing scheme: For $6,99 a month or, alternatively, US $ 59,98 a year, subscribers are allowed to access a library of more than a million tracks and a number of digital radio stations. In case they decide to own a particular track, they are billed a mere 79 cents per. Additionally, files are sharable via instant messenger with other members in the Yahoo! subscription community. Availability to date: United States only.

According to a study sponsored by the Online Publishers Association, more than 60 % of subscription consumers of digital entertainment content decide for a monthly contract (Online Publishers Association 2005). It remains to be seen whether or not Yahoo!'s low annual fee will change that behaviour.

Up- and downsides

The consumer: External devices are much cheaper to fill via a subscription than using individual downloads. Discovering new artists and styles is easy and painless, as you can listen to songs full-length without having to pay for each of them. Some think this is the next-generation radio (Leonhard and Kusek 2005; for a take on Yahoo!'s subscription service being in fact ad-sponsored web radio, see Malik 2005).

It can be argued that subscription services also fulfil people's need for belonging. Subscribing to a service, they become members of a club or community, not only customers of a shop. On the other hand, consumers may prefer single transactions with different shops and not binding themselves to one single online point-of-sale.

But there are disadvantages. Customers do not own the music they have paid for. If they cancel the subscription, the files become useless. This ultimately is a psychological problem, which is owed to the idea of "owning" music bought on physical media or from a download music store (Palmer 2005). Others say that owning music bought online is just a myth, as users are ultimately not in control of what they can do with the music they have purchased – e.g. burn as often as they want, share with friends and family, etc. (Leonhard and Kusek 2005).

Also, the collection of music can be less concise in case of subscription libraries. This is due to the fact that not the entire catalogue is available both for subscription and for purchase. For example, Rhapsody has 600,000 tracks available in the subscription section,

while the music store offers only 500,000 (Garrity 2004). Thus, the customer cannot be sure in every case that the song he or she wants to buy really is available.

The consumers' sceptical attitude is reflected by results of an INDICARE-survey, in the course of which consumers state that they would rather pay 1 Euro for a song that they can listen to as long as they like vs. 20 cents for a song they can listen to for one month only (read: subscribe).

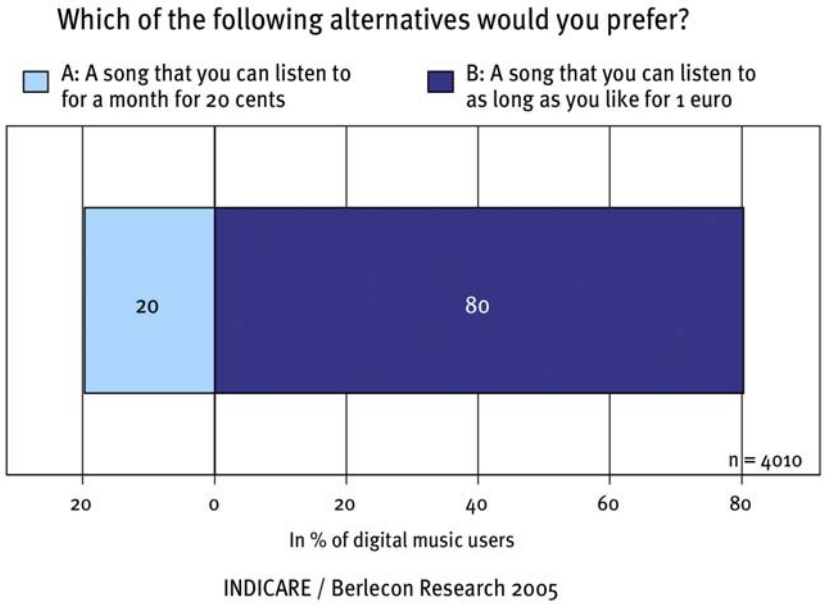


Figure 2: Willingness to pay for ownership (Europe)

A survey conducted in the USA asked consumers whether they prefer to buy tracks for US $ 1 each or pay a US $ 10 monthly subscription fee: 40 % chose to pay per track vs. 8 % would rather subscribe (Parks Associates 2005).

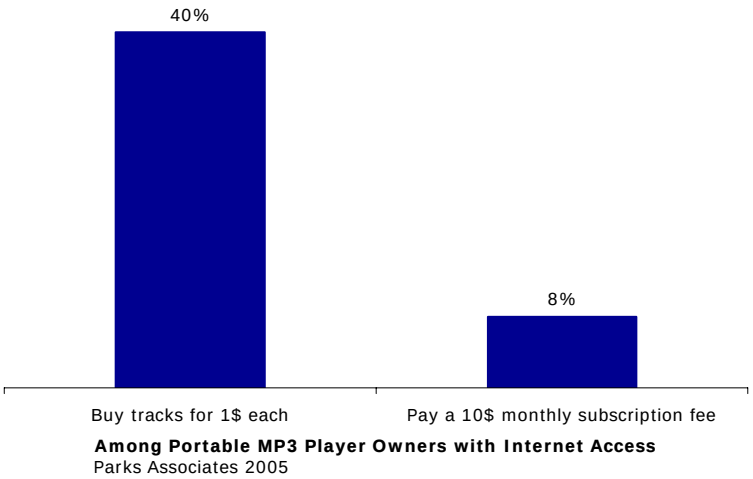


Figure 3: Willingness to pay for ownership (United States)

Subscribing to music is not yet a common idea with consumers. Especially the European market does not appear to be ready for that service. There is only Napster offering subscription in the United Kingdom and some smaller players like UK's Wippit.

Online Retailers: One of the greatest advantages is a constant revenue stream derived from subscription fees. This considerably reduces economic uncertainty and risk. Subscriptions are also more profitable for them, as revenues usually are split evenly between

the record labels and retailers. In the pay-per-track world, about 65 to 70 cents for each 99 cents are transferred to the record companies (Hansell 2004).

Furthermore, subscription services can be cross-selling opportunities. If the subscriber feels positive about the service, he will probably be willing to buy special releases, previews, package deals, tickets, merchandise, videos, books, etc. (Leonhard and Kusek 2005).

But there seems to be quite a long way ahead, as retailers need to work on two major issues: DRM and interoperability. Limited usage rights being the prime obstacle, the educational challenge is higher. It can be doubted that customers want to be educated about anything they spend their money on.

Also, there seems to be a severe misconception when it comes to DRM-awareness: Consumers do not know about it and if they do, they do not care too much (Dufft 2005). Napster's CEO, *Chris Gorog*, possibly misinterprets reality when stating: "As we market to the consumer that has not yet discovered digital music, he'll be going out and purchasing his first MP3 player, and in all likelihood, he'll want to make darn sure it's Janus-compatible". He or she hardly knows about DRM, let alone Janus DRM.

Also, retailers should make sure not to end up with a "razor and blade" business model (think Gillette), forcing the consumer to stick with a single soft- or hardware if the tracks are supposed to remain playable. Some argue that ultimately online music stores sell hardware, rather than music (Leonhard and Kusek 2005). For example, you cannot play tracks purchased from Napster on an iPod due to different DRM regimes; or you must use Yahoo!'s software to access its store.

Music labels: Music subscriptions first of all are another distribution channel. For some, it is even the "single greatest defence against piracy, because it most replicates the illegal experience of unlimited access to music" (Chris Gorog).

Given the fact that customers do not have to pay for each track, subscription models are a great platform to promote and expose less known artists. This can significantly increase track plays, the most important measure of success in the industry.

If the record companies are aware of their customers' perception and need for convenience, subscription services are a great promotional and distributional tool. As holds true for the online retailers, subscription reduces risk and uncertainty by generating a constant stream of revenue.

Conclusion

Subscription services can deliver real value to all stakeholders. Consumers are given access to large libraries of their favourite music; they do not have to pay separately for songs they want to listen to only a limited number of times; it is convenient when it comes to billing and it is cheaper than à la carte.

Online retailers and labels must realize that the biggest challenge is to make consumers comfortable with renting, as opposed to owning, music. They must also be aware that consumers do not care about DRM, but simply want to listen to music. Rights protection being essential for the success of music subscription, success can only come with smart and convenient business models.

In the end, subscriptions as well as commercial downloads compete with DRM-free music files that are perfect goods: they are available anytime, anyplace and without limitations. Some authors say that any cuts from that should be compensated by reductions in price or value-added services (Knopf and Sorge 2003). Others think that every accommodation short of total DRM-protection should be compensated by the consumer (Hansell 2004).

Bottom line

There will only be limited resistance on the side of consumers once prices drop, DRM-issues are resolved, and libraries are filled with millions of easily accessible tracks, which are interoperable with a multitude of inexpensive playback devices.

Sources

- Banerjee, Scott and Garrity, Brian (2004): Subs may best downloads. In: Billboard, Vol. 116, I. 35, p. 9
- Dufft, Nicole, et al. (2005): Digital music usage and DRM – Results from a European consumer survey. Online available at: http://www.berlecon.de/research/reports.php?we_objectID=224
- Garrity, Brian (2004): Song plays is the ultimate test for the health of subscriptions, A Q&A With Rob Glaser. In: Billboard, Vol. 116, Issue 16, p. 78
- Guth, Susanne (2003): A sample DRM system. In: Becker, Eberhard; Buhse, Willms; Günnewig, Dirk; Rump, Niels (Eds.): Digital Rights Management, Springer, Berlin Heidelberg New York 2003, p. 151
- Hansell, Saul (2004): Music sites ask, Why buy if you can rent ?. In: New York Times, 09.27.2004, Section C, p. 1
- Hellweg, Eric (2005): Music unlimited. In: PC World, Vol. 23, Issue 3, p. 4
- Knopf, Dominik and Sorge, Christoph (2003): Model-oriented analysis of user – right holder relations and possible impacts of DRM. In: Information Services & Uses, Vol. 23, Issue 4, p. 238
- Leonhard, Gerd and Kusek, Dave (2005): To own or not to own. In: Billboard, Vol. 117, Issue 16, p. 10
- Malik, Om (2005): The Yahoo music business model. Online available at: http://gigaom.com/2005/05/25/steve-jerry-and-the-yahoo-music-business-model/
- Online Publishers Association: Paid online content U.S. market spending Report, FY 2004. Online available at: http://www.online-publishers.org/?pg=opa_rsrch&dt=5
- Palmer, Jimmy (2005): Rent, lease, or buy – Which model is right for you?. Online available at: http://www.drmblog.com/index.php?/archives/60_Rent,_Lease,_or_Buy_-_Which_Model_Is_Right_For_You.html
- Parks Associates (2005): Global digital living. In: EContent, Vol. 28, Issue 4, p. 16
- Seff, Jonathan (2005): Napster's bad math. In: Macworld, Vol. 22, Issue 5, p. 20

About the author: After having graduated from University of Mannheim (Business Administration), *Philipp Bohn* has joined Berlecon Research as Junior Analyst. He is a member of the INIDICARE-team. Contact: pb@berlecon.de

Status: first posted 21/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=112

P2P sharing: Commercialize it!

By Philipp Bohn, Berlecon Research, Berlin. Germany

Abstract: The eminent rise and popularity of P2P networks such as KaZaA show that there is massive demand for conveniently shareable content. This challenges the success and business models of major media companies. Recent research shows that consumers are in fact willing to pay for the right to share files. This article identifies and evaluates business models from the particular perspective if and how peers are allowed to legally share purchased digital music. Business models based on legal P2P and sharing can be to the benefit of both the industry and the customer.

Keywords: economic analysis – business models, consumer behaviour, file sharing, P2P

What's the price for freedom?

Beyond doubt, some features of illegal P2P networks – such as taste-making and optimized delivery – are desirable for legal services (cf. Rosenblatt 2004). But considering the divergent interests of the entertainment industry, providers of P2P technologies and consumers, it seems hard to imagine how those features can be commercialized. In view of the copyrights concerned and the vastness of P2P networks, efficient tracking and billing of shared files is a complex issue. Yet, the idea that P2P sharing and commercial distribution of music continue to converge is supported by the results of the first INDICARE survey, which have recently

been made available (Dufft et al. 2005). This article provides an overview of the ecosystem of legal P2P and sharing models. In the course of this article, a P2P-network is understood to be a decentralized network that does not rely on a server-client infrastructure, circumventing third parties such as online stores. Sharing is the activity of making digital content available to peers.

The business of sharing

This article looks at existing and potential business models for sharing from two major angles: online vs. offline connectivity and distributional concepts that allow for sharing content. Before venturing on the details of sharing, an important distinction should be made concerning two prominent features of digital distribution. Its purpose can be primarily the sharing of content or the recommendation of music. While the industry embraces the latter, it is reluctant to provide ways to legally share copyrighted material.

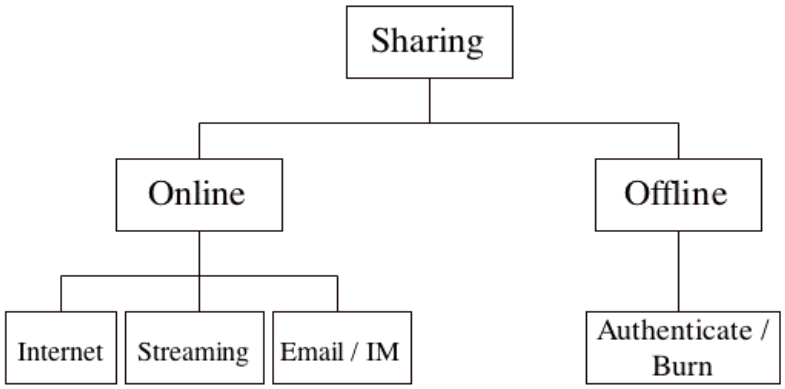


Figure 1: Online vs. offline sharing

Digital channels

The most prominent distinction is online vs. offline sharing (see Figure 1). If customers wish to exchange data online, they may chose – first of all – the Internet to up- and download content. In this case, sources comprise online stores, links on websites and blogs – both commercial and private – or file sharing networks. A second option is streaming. In this case there is no permanent download. Rather, content can only be consumed once. Applications such as Apple's iTunes make use of this technology. iTunes users located within a well-defined subnet (a division of a computer network) of up to five peers can browse and stream each other's musical libraries. A third channel in the online domain is email and instant messaging (IM). Peers send each other single files or playlists that the recipient is free to sample for a definite number of times. After that, he is invited to purchase the desired tracks for a fee.

Sharing is possible offline by means of simply burning a track to CD or DVD and physically handing it over to a friend. Most online distributors allow for burning songs a number of times. After that, DRM restricts further burning. There are also business models built on physical DRM-free distribution. In that case, consumers are encouraged to copy promotional CDs and share them with peers (Reynolds 2005).

Legal P2P business models

Business models can be divided into those that build on "bulk" or "individual" sharing. Generally, a P2P network is a decentralized network that does not rely on a server-client infrastructure. Bulk sharing models make use of the most prominent features of file sharing networks such as Ares, FastTrack, Overnet or Gnutella: consumers can browse enormous libraries of digital content and conveniently share it with peers. On the other hand, consumers may want to package and share

their music on a more personal basis. This usually happens via streaming but also by downloading and forwarding files (Gasser, McGuire, et al. 2005). In the case of business models for sharing, legal means the exchange of digital content without the violation of copyrights.

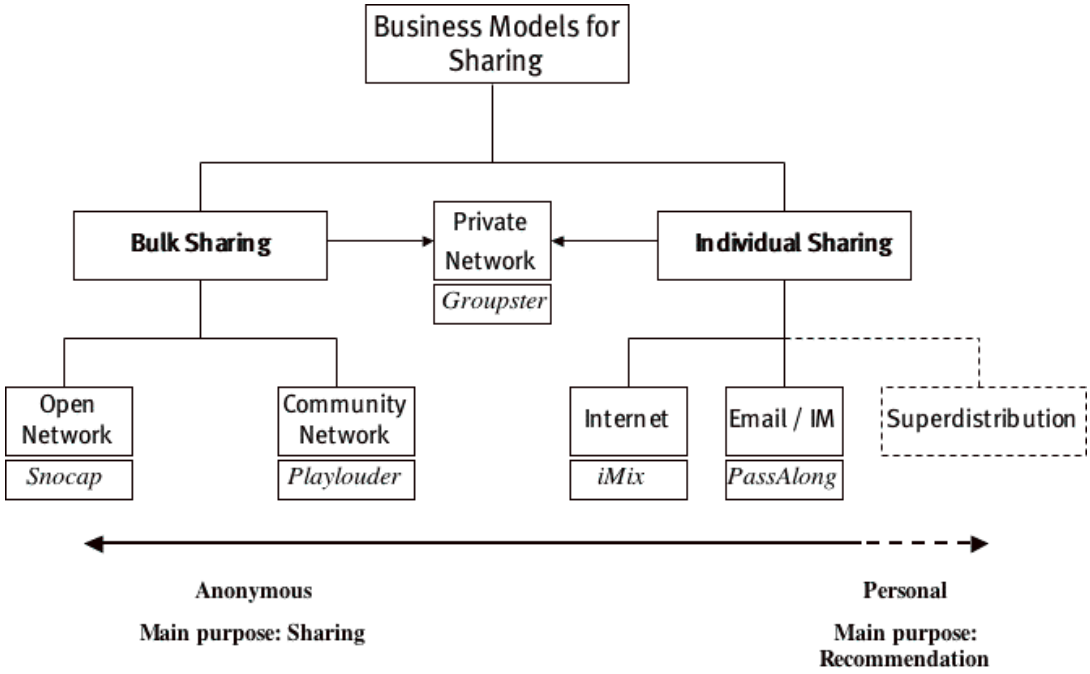


Figure 2: Business models from a sharing perspective

We can further differentiate bulk sharing between open networks and community networks, often referred to as "walled gardens" because of their exclusive nature. One of the most distinguished business models that make use of already existing open networks is Snocap. This back-end technology offers a licensing service that can be integrated into any P2P network service, e.g. KaZaA. Copyright owners can register their content in the company's database. They can then specify pricing and DRM (Jones 2004, Dean 2005). Former Grokster president Wayne Rosso's newly introduced Mashboxx service also uses Snocap to identify copyrighted tracks within networks like eDonkey and Gnutella (Adegoke 2004). Community networks such as UK's Playlouder MSP (MSP stands for Music Service Provider) offer the end user a bundle consisting of broadband Internet access and a library of musical content that can freely be shared among peers subscribing to that service. They cannot share with outside peers, though (hence, walled garden).

Individual sharing business models

On the other hand, consumers may want to package and share their music in a more personal fashion. In contrast to bulk sharing, individual sharing models focus more on recommendations. In the legal sharing environment, users are free to individually share single tracks or compilations of their favourite music. One example is iTunes' iMix feature. Anyone using iTunes can compile track-lists and share them via email or post them on the iTunes Music Store. Thus, friends and peers are invited to browse and sample previews of music recommended to them for free and eventually make a purchase. There are other schemes that make use of email and IM services to allow customers to share content. PassAlong Networks has partnered up with eBay and offers a library of about 200,000 songs available to forward via IM. Likewise, MSN Music Store allows using MSN Messenger to share music (Gasser, McGuire, et. al. 2005).

Yahoo!'s Music Unlimited service, that has just been launched in beta mode in the U.S.,

is also based on the legal sharing concept. In contrast to competing, more expensive offers, sharing with peers does not seem to be a mere accommodation. It rather stands at the core of the service. Sharing options are heavily integrated into Yahoo's own messenger and desktop application. Subscribers may freely access, browse and stream each other's library or send music files to other subscribers via the company's own messenger (it is possible for the customers to opt out of the sharing features). The company obviously came to realize that one of the most important factors of commercial success is community building (Dean 2005).

There are also superdistribution models or promotional networks like Altnet's PeerPoint Manager (PPM) that offer incentives to share specific content. These offers are primarily distributional or promotional tools. Participants collect points per file they share. They may then redeem those points for content or win prizes.

Finally, there is a grey area in between bulk and individual sharing. Applications such as Groupster allow peers to form individual sharing communities. Each member has to be authenticated within the network. Once done, members can freely share all the content they wish – including of course digital music. As individual communities are limited to 30 members and mp3 files can only be streamed, this is argued to fall under the fair use exemption (in the US copyright environment, that is). This clause allows copyrighted material to be shared with a private audience, such as close friends and family (Metz 2005).

What's the motivation to engage in P2P?

There are two major reasons for content providers to offer P2P features: reduction of distributional costs and recommendation of content. Distribution costs for musical content are only 20 cents for each dollar spent on traditional distribution, e.g. via CD (Palenchar 2005). Furthermore, for some companies P2P distribution might also be a way to cut down on costs for server and broadband capacity, as there is no need for a centralized infrastructure (heise online 2005). Opportunities to save on costs make P2P very attractive especially for independent labels that command slimmer marketing budgets than the majors.

Traditionally prone to mass marketing, sharing and recommendation schemes give major music labels the chance to get down to the personal level. EMI UK's chairman and CEO *Tony Wadsworth*: "As a concept, any thinking person can see that customers turning other people on to music can be a good thing" (Anon. 2004). This holds true especially for legal sharing, which is less anonymous than P2P (please refer to Figure 2).

Another important advantage of P2P and sharing is long-tail distribution. This concept states that products that are in low demand can make a substantial market if only the distribution channel is large enough. Those items may eventually outsell current bestsellers and blockbusters. Given the global penetration of broadband networks, labels are now given the opportunity to sell content that would be too expensive to distribute using traditional channels and targeting smaller audiences (see Anderson 2004 for an introduction to that concept).

Conclusion

The commercialization of P2P sharing offers potential benefits for consumers and the industry alike. P2P sharing offers cheap distribution channels. There are innovative ways to distribute content that formerly was too expensive using traditional distribution. From the consumers´ perspective, P2P gives them the opportunity to conveniently share digital content at any time. Furthermore, it is a way to obtain recommendations from trusted personal sources as opposed to anonymous marketing messages. Finally, if the right-holders themselves seed their content into P2P networks, the number of intentionally corrupted files and spoofs will be reduced. This leads to an increase in content quality and attractiveness of commercial P2P sharing.

On the downside, consumers can only chose between various technologies, services, concepts and platforms that are mostly incompatible. Even if the consumer has worked through that thicket to decide on a service

that suits his specific needs and consumption behaviours, he cannot get in touch with peers outside the particular network. Bundled offers or services tied to certain devices make sense only so far as they strengthen DRM but limit consumers' flexibility.

Bottom line

The fact that digital rights need to be protected and artists to be paid is essential and unquestionable. With a convenient and efficient DRM system handled by back-end technology and business models that centre around consumers' needs and preserving community spirit within the sharing network is a promising way to success.

Sources

- Adegoke, Yinka (2004) : Record labels find a way to work with P2P. In : New Media Age, 11.11.2004, p. 12
- Anonymous (2004) : New filesharing set-up to reward legit users. In : Music Week, 14.06.2004, p. 6
- Anonymous (2004) : Legal P2P services gather steam. In : Music Week, 16.10.2004, p. 5
- Anderson, Chris (2004) : The long tail. In : Wired 12.10. Online available at : http://www.wired.com/wired/archive/12.10/tail.html
- Dean, Katie (2004): Napster star changes his tune. In: Wired News, Dec. 03, http://www.wired.com/news/digiwood/0,1412,65893,00.html
- Dean, Katie (2005): Music mis-match. Wired News, May 12, http://www.wired.com/news/digiwood/0,1412,67495,00.html?tw=wn_tophead_2
- Dufft, Nicole et. al. (2005): Digital music usage and DRM – Result from an European consumer survey. Online available at: http://www.indicare.org/survey
- Gasser, Urs, McGuire, Mike, et. al. (2005): Copyright and digital media in a post-Napster world. The Berkman Center for Internet & Society at Harvard Law School. Online available at http://cyber.law.harvard.edu/home/uploads/254/2003-05.pdf
- heise online (2005): Bertelsmann-Tochter plant Distributionsplattform mit P2P-Technik, 22.03.2005. Online available at: http://www.heise.de/newsticker/meldung/57805
- Metz, Cade (2005): P2P Goes private. In: PC Magazine, Vol. 24, Issue 2, pp. 96 – 102
- OECD Committee For Information, Computer and Communicatins Policy (2005): Digital Broadband Content: Music. Online available at: http://www.oecd.org/document/46/0,2340,en_2649_201185_34994926_ 1_1_1_1,00.html
- Palenchar, Joseph (2005): Prophets: music-industry judgement day near. In: TWICE – This Week in Consumer Electronics, Vol. 20, Issue 7, p. 14
- Reynolds, Rob (2005): Spreading the word for free. In: Music Week, 09.04.2005, p. 20
- Rosenblatt, Bill (2004): Learning from P2P: Evolution of business models for online content. INDICARE Monitor, Vol. 1, No 6/7. Online available at: http://www.indicare.org/tiki-read_article.php?articleId=61
- Talbot, Martin (2005): Firms line up to launch file sharing offering. In: Music Week, 05.02.2005, p. 7

About the author: After having graduated from University of Mannheim (Business Administration), *Philipp Bohn* has joined Berlecon Research as Junior Analyst. He is a member of the INIDICARE-team. Contact: pb@berlecon.de

Status: first posted 23/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=115

Digital Media Project – Part I

Towards an interoperable DRM platform

By: Ernő Jeges, SEARCH Laboratory, Budapest, Hungary

Abstract: The Digital Media Project, often referred to as DMP, is the fruit of a grass root movement that developed in 2003. Its main aim is to develop the fundamentals of standardized and interoperable Digital Rights Management for digital media. Although the project is making publicly available numerous documents on its website (DMP web site 2005), it is not easy to put the pieces together and to assess the project. Therefore INDICARE dedicates a two part article to DMP. The present first part aims to give a brief overview of DMP and its approach, while the second part – scheduled for the next issue of the INDICARE Monitor – will attempt a critical assessment.

Keywords: review – consumer rights, digital media, fair use, interoperability, stakeholders, standards

Introduction

Ever since content has existed, it had to be carried by some physical media, making possible the handling (viewing, listening, etc.) of the content by some appropriate physical device. In the age of the analogue media the connection between these two levels, the content and its handling technology was very tight, as the usage of the media always materially affected the content. This way the distinction between the medium and the content itself was blurred. This circumstance has strongly influenced the evolution of the media business, policies and legislation, and has shaped the form in which these issues exist today.

With the appearance of digital media, both the existing functionalities of the analogue media were extended and a wider set of functionalities was made possible. The Digital Media Manifesto (Manifesto 2003) calls this new experience, offered by the digital technology the Digital Media Experience. However, as the business and legislative models draw their origin from the analogue world, many practical solutions are lacking, and what is worse, some of new and innovative models appeared to be unprofitable or, sometimes even had to face legal prosecution.

This stalemate has both economic and social consequences. As digital media has the potential to become the major driver e.g. for the spreading of broadband access, or for the development of consumer electronics and the IT market, these industrial domains suffer vast economical damage from the stalemate on digital media. From the social point of view, further development of digital media could enhance education, information interchange and the overall well-being of individuals.

The vision of DMP is to break the stalemate regarding digital media: "*The Digital Media Manifesto proposes to make an improved Digital Media Experience economically rewarding on a global scale, legitimate for the multiplicity of players on the value-chain and satisfactory for end-users, with the ultimate goal of realising a fuller Digital Media Experience*".

The Digital Media Project members – at present DMP is an organisation with members from circa 20 companies from all around the world –, have realized that the key for achieving this goal is in standardising DRM technology. By having a widely accepted standard for the whole DRM value-chain, the services and the devices would exploit the possibilities of the digital media more efficiently, thus not only promoting the acceptance of these technologies among the end-users, but also motivating the content creators to use digital technologies as new, inspiring media to distribute their work, relying on a dependable remuneration system.

From decomposition to interoperability

In the terminology of DMP (Terminology, 2005), all actors in the value-chain, irrespective of being at the beginning, somewhere in the middle or at the end of the chain are called *users*. The consumers, as the actors at the end of the value-chain are called *end-users*. Users perform certain *functions* to do business between each other. Functions are implemented using *tools*, which represent the underlying technologies that handle the digital media. The following figure shows the value chain as identified by the DMP (Architecture, 2005):

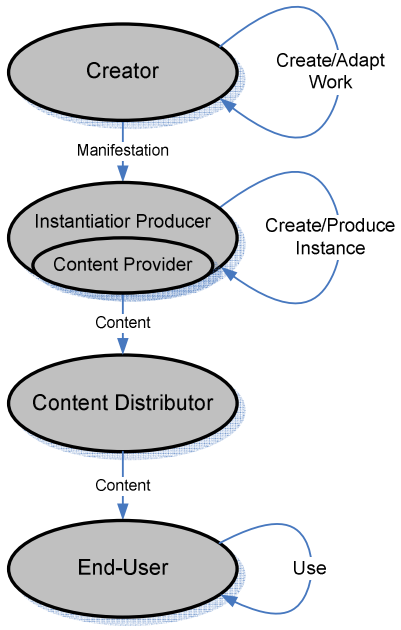


Figure 1: Digital media value-chain

The technology, thus including the underlying tools, is changing very rapidly, so it cannot be guaranteed that a function that has been used recently, or is used today in the value-chain, will exist unchanged for a longer period of time. For this reason, identified functions were decomposed into atomistic *primitive functions*, which, appeared to be quite stable from an examination of the development of both analogue and recent digital technologies. As they were constantly present in different functions throughout the continuously developing technologies, it was obvious that standardisation could be achieved by the standardisation of these primitive functions. In this way, any future function could be either composed using the already standardized primitive functions, or a new primitive function would have to be introduced, without modifying the original architecture of the standard. Primitive functions describe simple activities like for example "Identify data", "Authenticate user", or probably the most evident "Access content" (IDP Functions and Requirements, 2005).

The primitive functions are derived from the complex functions being used in today's tools, which are on the other hand identified by examining several media usage scenarios, called *use cases* (Use Cases, 2005). As the use cases are based on the digital technologies in the form they exist today, or are planned to exist in the future, their analysis could result in DRM solutions that would alter the evolved balance between different users in the value-chain and modify the way they usually do or have done their mutual business. To prevent this effect, DMP has constructed an imposing list of 88 *Traditional Rights and Usages* (TRU-s). These rights and usages are used as guards to test whether standardised DRM technology would violate the scope of traditional expectations of different users in the value-chain, especially the end-users. As people's expectations about DRM solutions are based on their present and past experiences, this is an effective way to ensure that a proposed DRM solution would not force the users against their needs, thus keeping the proposed DMP standard future-proof.

After having the past, the present and the future planned tools decomposed to the level of primitive functions, DMP has a level playing field, in which new standard tools can be assembled. The set of standardised DRM tools based on the primitive functions is a toolkit called the *Interoperable DRM Platform (IDP)*, whose specification is the most important technical outcome planned by the Digital Media Project (Interoperable DRM Platform, 2005). This toolkit could provide both lightweight and heavyweight DRM solutions, depending of the specific needs (Chiariglione's Vision, 2004).

In the terms of the DMP, interoperability means the ability of the users in the value-chain to execute functions using standardised tools, which have open specifications and are independently implemented. The IDP not only provides potential to implement a great variety of value-chains using standard technologies, but these value-chains also remain compatible, as they are built up from interoperable tools. Furthermore, lower prices and higher level of services are expected for the benefit of the end-users, not only because of the reusability of the standard tools, but because of the higher level of competition between different device manufacturers and service providers, as both the tools and different services could be supplied by multiple, competing parties.

These properties envision, that IDP may release the tension between interoperability and information security described in (cf. van Daalen 2004). In the terms of the DMP every manufacturer is applying pieces from the same "democratic" standard, as there are no producers which can be called "third-parties", who can be admitted to or barred from the market, and the regulation of DRM solutions is not enforced by governments, but the standard alone. Competing producers on the market can really concentrate on the services their devices offer, knowing, that the underlying interoperable DRM solution is secure enough to protect the contents.

The role Traditional Rights and Usages

There are several actors in the value-chain, having different interests. Diffusion of a standard technology is highly influenced by having the proper respect of the rights of every value-chain member. In fact it is an important aspect of standardization to decide which functions and rights should be mandatory in the standard, and which should be left open to negotiations between different value-chain users. However meeting the end-users' expectations has the most important role in fostering the acceptance of a DRM solution.

To achieve this goal, DMP has stated that both technological and legal aspects of DRM need the existing policies to be revised. From the legal point of view maybe the most important, but merely general stated goal is that basic user rights, as traditionally enjoyed by end-users should be ensured. The list of Traditional Rights and Usages is an irreplaceable tool in being attentive to this goal, as DMP not only improves the support of TRUs by describing scenarios of how these rights and usages could be supported, but is also deriving additional Tools and Use Cases from scenarios, to see, whether present demands can be fulfilled relying on the standard being developed. Being successful in this would mean that presumably any future demand would also be met.

On the other hand, from the purely technological point of view, several main features are defined, which a widely accepted DRM solution must provide. Beside the requirement that all users in the value chain must have technical ability to access the standardized DRM platform, and that this access should be done with a single device for similar services, it is also stated that the rights and usages traditionally enjoyed by end-users should be technically supported.

As for "fair use", being an essential traditional use enjoyed by end-users, the DMP terminology does not talk about the right to copy content for one's own purposes, but it speaks generally about the "ability to make continued access", which is again more general, but also more abiding. This includes the "right to time shift" or the "right to space shift" content, which mean respectively to access "owned" content anytime and anywhere.

Based on their origin, Traditional Rights and Usages are classified into the following groups:

- Already-established legislative TRUs of content creators and end-users.
- Commercial and remuneration TRUs of direct economic significance.
- TRUs related to general social liberties.
- Fundamental TRUs from historical practice and interaction with analogue media.
- Consumer-choice TRUs relevant to the high-tech environment.

So, basically, TRUs are here as safeguards, to protect DMP from derailing; however, an identified, defined and described TRU does not necessary mean, that a user *should have* a right to use the digital media in the specified way, but it only indicates that different value-chain users, especially the end-users would probably be *interested* in using the digital media in the same way. TRUs simply express the users *expectations*, which may change very slowly compared to the technology, but respecting them has an ultimate role in the acceptance of a DRM standard.

Bottom line

At the present state of its work the DMP has released a Call for Contributions "Mapping of Traditional Rights and Usages to the Digital Space" (Call for Contributions, 2005). In this call the DMP is expecting contributors to define, in what form Traditional Rights and Usages could be supported by the Interoperable DRM Platform. Several most important rights and usages are chosen from the list of TRUs, and as a result of this process, Recommended Actions will be developed that are to be presented to governments and regulators. Having presented the basics in this article, in the next issue of the INDICARE Monitor we will try to figure out the pros and cons of the DMP approach

Sources

- Architecture (Technical Reference, Approved Document No. 2), 15/04/2005; http://www.dmpf.org/open/dmp0402.doc
- Call for Contributions on "Mapping of Traditional Rights and Usages to the Digital Space", 15/04/2005: http://www.dmpf.org/project/ga06/TRUCfC.htm
- Chiariglione (2004): Chiariglione's vision: An interoperable DRM platform to the benefit of all. INDICARE-Interview by Knud Böhle. INDICARE Monitor, Vol. 1, No 6/7, December 2004; http://www.indicare.org/tiki-read_article.php?articleId=58
- Interoperable DRM Platform (IDP) Functions and Requirements, 28/01/2005; http://www.dmpf.org/open/dmp0328.doc
- Interoperable DRM Platform (Technical Specification, Approved Document No. 3), 15/04/2005; http://www.dmpf.org/open/dmp0403.doc
- Terminology (Technical Reference, Approved Document No. 6), 15/04/2005; http://www.dmpf.org/open/dmp0406.doc
- The Digital Media Manifesto, 30/09/2003; http://www.dmpf.org/open/dmp0022.doc
- The Digital Media Project web site, 2005: http://www.dmpf.org
- van Daalen, Ot (2004): The tension between interoperability and information security, INDICARE Monitor Vol. 1, No 3, August 2004; http://www.indicare.org/tiki-read_article.php?articleId=36
- Use Cases (Technical Reference, Approved Document No. 1), 15/04/2005; http://www.dmpf.org/open/dmp0401.doc

About the author: *Ernő Jeges* is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His research areas are mainly focused on biometric security solutions, but he was involved in a number of research activities dealing with IT security and the technology aspects of digital rights. He received an MSc in computer science from BUTE in 1995. Contact: jeges@mit.bme.hu.

Status: first posted 23/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=116

DRM: from theory to implementations

Report from a course in Louvain-la-Neuve, 17-19 May 2005

By: Ernő Jeges, SEARCH Laboratory, Budapest, Hungary

Abstract: This is a report from the course "Digital Rights Management – from theory to implementations" organized by the Graduate School in Electronics and Communications at Université catholique de Louvain in Louvain-la-Neuve, Belgium. It was a three-day course from 17th to 19th May, 2005, focusing on different technical aspects of DRM, like watermarking and steganography as means of data hiding in digital contents, key management and traitor tracing in digital broadcasting systems and much more.

Keywords: conference report – digital broadcasting, technical protection measures, watermarking

Introduction

The Graduate School in Electronics and Communications (GSEC) at the Université catholique de Louvain (UCL) is co-organized by three UCL laboratories from the Electrical Engineering Department (ELEC). The courses of the GSEC are provided both to gain background knowledge of different areas, and to gain an understanding of the latest research. The course "Digital Rights Management – from theory to implementations" had the technological aspects of DRM systems in its focus (AS13). The majority of attendees were from UCL and other Belgian universities, but as the course was open to the public, and the list of invited speakers offered a promising overview of the latest results in the area, a great number of people had registered to the course from all around Europe.

The three-day course started with a brief introduction to the cryptological basis of the technologies widely used in DRM systems, which was held by *Jean-Jacques Quisquater* and *François Koeune*, the hosts of the course. Their lectures included topics like symmetric and asymmetric cryptography, RSA encryption and digital signatures, key exchange protocols, data hashing and the set-up of public key infrastructures.

Introduction to watermarking

After the quick mathematical warm-up, we were thrown into the deep water of watermarking by *Ingemar Cox* from UCL (this time this abbreviation means the University College London). First of all, the definition of watermarking and several related terms were given (Cox).

Watermarking is the practice of unobtrusively modifying a work of art (image, song, software program, geometric model, etc.) to embed a message *about that work*. This is considered a general definition, and may differ from other definitions, which may include also imperceptibility, or can refer to any means of data hiding. Following this train of thought, we defined *data hiding* as a general technology for preventing adversaries from perceiving or finding some kind of data, and *steganography* as keeping the existence of messages secret by hiding them within objects, media, or other messages. So, to simplify, hiding data in (digital) content is the goal, and if the embedded information is about the carrier content itself, then it is watermarking, but if it is an arbitrary secret message then we call it steganography.

To detect the embedded watermark, we can either use some information about the original, unmodified content (*informed detection*), or not (*blind* or *uninformed detection*). The error rates in watermark detection can be expressed using the *false positive rate*, as a frequency with which we can expect to find watermarks in content that is not watermarked; and the *false negative rate*, the frequency with which we can expect *not* to detect watermarks in watermarked works. The acceptable level of these error rates depends of the particular application.

The most important properties of watermarking systems are:

- *Fidelity* – the perceptual similarity between marked and unmarked works.
- *Payload* – the amount of information that a watermark can embed in a single work.
- *Robustness* – the watermark's ability to survive normal processing (e.g. compression).
- *Security* – the scheme's ability to resist hostile attacks, specifically designed to defeat the purpose of the watermark.

In DRM systems the most common goal of watermarking is to imperceptibly and irremovably include information about the content in the content itself for the purpose of broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication or copy control.

Applications

The first speaker of the second day was *Adi Shamir*, who is presumably often introduced as "the S from RSA", just as happened this time. He presented a key management scheme in broadcasting systems, where we have to address a *privileged subset* of end-users by broadcasting encrypted content to them using multiple pre-distributed keys. The schemes introduced in the talk were based on a binary-tree with the end-users on the leaves; we can define inclusions and exclusion of sub-trees on the branching nodes, to choose the right keys to have the desired subset of end-users being able to access the content. The latest improvement in this technique is the LSD broadcast encryption scheme (Halevy and Shamir 2002).

After the later mentioned panel discussion we had a lecture by *Yvo Desmedt*, who was speaking about traitor tracing in broadcasting environments. The goal is to find the subscriber or maybe some conspiring subscribers, who extract their keys from their devices (e.g. a set-top-box) to sell them on the black market. Several schemes were introduced, discussing their strengths and weaknesses. The speaker concluded, that traitor tracing is a useful tool for DRM, especially in broadband broadcasting, and is becoming better and better, but there are some limitations: for example there is a proven theorem, that a *perfect* traitor tracing scheme (where an *innocent* party is *never accused*) is impossible (cf. Desmedt et a.l. 2002).

As nowadays more and more digital applications, like first-person-shooting games, medical images, different simulations and computer aided design (CAD) systems rely on inner 3D object representation, it has became essential for product or service providers to protect their intellectual property inherent in these models. In the first lecture of the closing day a watermarking scheme was introduced, using which a secret message can be embedded in a 3D model. With the future appearance of 3D-televisions, this issue can be essential for content providers, and furthermore, a brave vision of a 3D-Google was sketched.

In the rest of the closing day a basic model for access control to content was introduced, after which the last lecture of the course introduced the digital cinema and its most important technical issues, focusing on the requirements and challenges of choosing hardware components based on which a robust and secure digital cinema hardware can be built.

The panel discussion

The panel discussion started with a "warm-up" question directed at *Adi Shamir*, questioning what's new in cryptography and cryptoanalysis. Mr. Shamir's feeling was that the cryptoanalysis of hash functions is an area, in which not much has happened since 1990's, and that research has received a boost lately.

As the majority of lectures focused on watermarking, the discussion concentrated on this issue. The greatest challenge in this area today is to develop *public-key watermarking* (PKWM), similarly to public-key cryptography, which would presumably mean that one can put watermarks on a piece of content using a private key, so that everybody would be able to check the existence of the watermark using a public key. As the word *presumably* in the last sentence indicates, the biggest problem is that we don't even have a precise definition or even a clear goal yet concerning the PKWM.

After a short debate it turned out, that our expectations in the area of classic watermarking are not clear as well. We are trying to trace the content by technical means, to find where it is leaking, but in the end in most cases it turns out that the leaking point is some old lady living in a small village, so the technical solution is barely handy. The speakers agreed that DRM is more about psychology, as a leak is not the cause of the problem, only the syndrome.

The problem in today's business models originates from the fact, that those who are putting protection on contents are not those who profit from really strong protection. A strong watermarking scheme, which is still a wish, could completely restructure currently failing business models, as in the future content providers will be able to put the needed protection in the content themselves. Still, the only thing that can be done by device manufacturers today is not to chose a standard now, but to build upgradeable devices, and to be prepared for constant improvement of the schemes, like it was in the case of smart cards used for phone-cards.

Before the end of the panel discussion, *consumer privacy* in broadcasting techniques was discussed. As broadcasting becomes more and more interactive, providers will be able to monitor consumers' activity. This backward information should also be covered in forthcoming DRM solutions, thus a strong demand for *two-way* DRM systems is arising, where not only the content providers' rights are ensured, but also the consumers' privacy is protected by technical means.

Conclusions

As a conclusion we can state that the main challenges to technical solutions of DRM are moving towards a risk management-based approach, admitting that piracy cannot be completely eliminated, but at least it must be controlled. Watermarking could be a useful tool in implementing these new protection schemes, which would need a change in the current business models. However watermarking is not strong enough yet to sustain possible attacks, and it is still questionable, whether it will ever reach the desired security and robustness level.

By the spreading of broadband access and digital broadcasting, the need for technical solutions to control both the broadcasted content and the backward information flow is growing. The panel discussion proved that in some areas research is demand-driven, but several areas are developing without clear definitions and a clear view of the possible usages, which is admittedly not necessarily a problem in the early phases of research.

Bottom line

As for the current state of DRM protection schemes, the summary of the panel discussion, addressing the attendees, can serve as the overall summary of the course: "Everything is broken, so we are waiting for your research". Not so promising, but at least optimistic.

Sources

- AS13 - Digital Rights Management: from theory to implementations: http://www.gsec.ucl.ac.be/AS13.php
- Cox, Ingemar J.: http://www.ee.ucl.ac.uk/~icox/
- Desmedt, Y.; Burmester, M.; Kurosawa, K. (2002) On Perfect Traitor Tracing, ISIT 2002: http://kuro.cis.ibaraki.ac.jp/~kurosawa/2002/ISIT02.pdf
- ELEC – Département d'électricité: http://www.elec.ucl.ac.be/
- GSEC - Graduate School in Electronics and Communications: http://www.gsec.ucl.ac.be/
- Halevy, D. and Shamir, A. (2002): The LSD broadcast encryption scheme, Advances in Cryptology – Crypto'02, Berlin, 2002, pp.47-60
- UCL – Université catholique de Louvain: http://www.ucl.ac.be/en/

About the author: *Ernő Jeges* is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His research areas are mainly focused on biometric security solutions, but he was involved in a number of research activities dealing with IT security and the technology aspects of digital rights. He received an MSc in computer science from BUTE in 1995. Contact: jeges@mit.bme.hu.

Status: first posted 23/06/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=114

Editorial of INDICARE Monitor Vol. 2, No 5, 29 July 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The articles in this issue comprise a prudent reply by Creative Commons to the polemic published in the June issue of the INDICARE Monitor, a tour d'horizon through European consumer protection laws in the light of digital products, and an outline of the recommendations by the Norwegian Board of Technology (NBT) on DRM to the Norwegian Parliament. Further we have included two market analyses, one on DRM in the eBook area, the other dealing with the podcasting scene. In addition there are two more technical contributions, one presenting the European FP6 project TIRAMISU and the other giving a detailed report about the second international ODRL workshop held this month in Lisbon.

Keywords: editorial – INDICARE

About this issue

Licenses, laws, and policy making

The issue starts with a cautious reply by intellectual property attorney *Mia Garlick*, General Counsel of Creative Commons Corporation, to the polemic "Creative Humbug" by *Péter Benjamin Tóth* (Tódt 2005), legal counsel at the Hungarian musical collecting society ARTISJUS. Mia's rebuttal of Tódt's attacks is very detailed as she substantiates her arguments with the latest facts and figures about Creative Commons and examples where Creative Commons has already been beneficial. In spite of all differences, she underlines that both, Creative Commons and collecting societies like ARTISJUS, are "working towards the same goals and representing, potentially, the very same individuals". I hope that this peace offer is not the end of debate about CC. A question which puzzles me for instance is if there is a path from CC licenses over encoding these licenses in rights expression languages (cf. ODRL 2005; cf. Guth et al. in this issue) to the enforcement of theses licenses by technical measures.

Legal ICT consultant *Martien Schaub* provides a breakdown of consumer protection laws in the light of digital products (which may come with DRM protection). Her tour d'horizon though European law touches upon six directives: Directive 85/374/EEC (liability for defective products), Directive 93/13/EEC (unfair terms in consumer contracts), Directive 97/7/EC (protection of consumers in respect of distance contracts), Directive1999/44/EC (sale of consumer goods and associated guarantees), Directive 2000/31/EC (e-commerce directive), and Directive 2005/29/EC (unfair business-to-consumer commercial practices). The legal provisions turn out to be fuzzy because what is lawful depends to a large extent on assumed reasonable *consumer expectations,* and by nature these vary with technical changes, learning processes, and differ between application fields. For example, some DRM controlled music offers might be accepted in the mobile environment, but be rejected in a PC environment or home entertainment domain. The best instrument to protect the consumer, she concludes, "appears to be the information duties of the seller. In case of lacking, inadequate or false information about the product, a consumer may successfully base a claim on breach of contract or unfair practices".

Christine Hafskjold who works for the Norwegian Board of Technology (NBT) reports about the results of a project on DRM which was intended to inform the Norwegian Parliament and policy makers in the process of amending the Norwegian Copyright Act. Meanwhile the act has passed (June 4th). The final act is in line with the recommendations given by NBT. The amendment is considered consumer friendly, underlining the right to make private copies and even allowing to circumvent technical protection measures in order to copy music from CDs to MP3-players. In the INDICARE Monitor of last month *Thomas Rieber-Mohn* (2005), University of Oslo, wrote specifically about the implementation of the EUCD Article 6 in

Norway. The two articles complement one another perfectly.

DRM in podcasting and eBooks

Nicole Dufft, from INDICARE partner Berlecon Research, draws attention to Podcasting, an amateur movement to use the expression of *Dan Hunter*, which is so successful that commercialization appears to be inevitable. Copyright and consequently DRM however is an issue. Nicole can imagine commercial, DRM-protected podcasts where DRM limits, for example, the number of plays and prevents the extraction of individual songs. The prime problem of such commercial offerings to be accepted by consumers will be the lacking interoperability of DRM solutions.

Philipp Bohn, Berlecon Research, takes a look at recent eBook developments, classifying first the devices able to run eBook software and to display eBook content, before he comes to widely diffused reader software, namely Adobe Acrobat, Microsoft Reader, eReader and Mobipocket. He is not convinced of the success of eBooks as long as interoperability matters are not solved, but he argues that in principle there are business models making DRM protected eBooks acceptable for consumers, e.g. he can imagine a demand in the educational environment for "term lease" or "course-packs" if they go together with price reductions. Who is likely to reads this article may also want to re-read *Karen Coyle's* (2005) article dealing with library lending of e-books in the USA.

Technical matters

The object of project TIRAMISU (The Innovative Rights and Access Management Interplatform Solution) is, according to its website, "to unleash the full potential of digital media, addressing the complete consumption chain – media creation, delivery and consumption, while removing the Digital Rights Management (DRM) barriers. TIRAMISU is an FP6 project sponsored by the European Commission. Consortium partners are Optibase, ARTTIC, Imperial College of London, Orange, NagraVision, Industrial Technology Research Institute ITRI (Taiwan), University of Ljubljana, Ecole Nationale Supérieure des Télécommunications ENST, France Telecom, and Fraunhofer-Gesellschaft.

What makes TIRAMISU particularly interesting for INDICARE is its claim to render unobtrusive DRM components. So we asked the project team to explain their approach and to reflect about barriers to success. In a few words: they target the "home domain" (authorized domain), support superdistribution, try to achieve increased security by the application of smartcards, and base their developments on open standards such as MPEG-21.

Those who are less interested in technology are encouraged to read at least the final section headed "Is TIRAMISU the next hot technology?" in which success factors, i.e. conditions to be accepted as a worldwide open international standard, are discussed.

Finally INDICARE informs you about the ODRL Workshop which took place in Lisbon in July. More precisely, the three program chairs of the workshop, *Susanne Guth*, *Renato Iannella*, and *Carlos Serrão*, give you their briefing.

Although the event focused on ODRL developments, many relevant topics of the general DRM debate were addressed. The need for interoperability and standardization clearly stimulates convergence and co-operation. The use of rights expression languages for identity management links them to Trusted Computing as the specification profile of ODRL for CC indicates co-operation with the commons oriented movement. In between are attempts to make rights expression languages "bi-directional" or to otherwise attach negotiations of rights to the exchange of assets. Pushed by the Open Mobile Alliance (OMA), convergence of DRM solutions from mobile over PCs to broadcast is on the agenda requiring co-operation to be successful.

Co-operation is without doubt on the agenda of the European Union striving to build ERA, the European Research Area. One instrument is the organisation of co-ordination meetings bringing together different 6th-Framework-Program (FP6) projects and activities. In the area of "Networked Audio Visual Systems

and Home Platforms" (NAVSHP), four different co-ordination groups have been established, one of them, CG1, is dealing with Digital Rights Management. It brings together members of six FP6 projects (Medianet, Enthrone, Tiramisu, Danae, Avista, and Visnet), FP5 project ELIN and the European Broadcasting Union. Together they work, chaired by *Leonardo Chiariglione,* on a "DRM Requirements Report that expresses the common view of NAVSHP on DRM and the requirements for future DRM technologies, systems and toolkits in the European audio-visual sector". This work is highly interesting for INDICARE, and hopefully for you. It will also be of interest to compare these requirements with the work in progress of the Digital Media Project aiming at "Recommended Actions" to be presented to governments and regulators (cf. Jeges 2005).

Bottom line

As always the INDICARE Monitor aims to stimulate debate and provoke online-comments through the articles provided. By the way, for the first time the leading authors of these articles are in their majority women.

Sources

- Coyle, Karen: The role of digital rights management in library lending. INDICARE Monitor, Vol. 2, No 2, 29 April 2005; http://www.indicare.org/tiki-read_article.php?articleId=95
- Jeges, Ernő: Digital Media Project – Part I. Towards an interoperable DRM platform. INDICARE Monitor, Vol. No 4, 24 June 2005; http://www.indicare.org/tiki-read_article.php?articleId=116
- ODRL (2005): ODRL Creative Commons Profile. Specification: 6 July 2005; http://odrl.net/Profiles/CC/SPEC.html
- Rieber-Mohn, Thomas: Norwegian implementation of the EUCD Article 6. INDICARE Monitor, Vol. No 4, 24 June 2005; http://www.indicare.org/tiki-read_article.php?articleId=111
- Tóth, Péter Benjamin: Creative Humbug. Personal feelings about the Creative Commons licenses INDICARE Monitor, Vol. No 4, 24 June 2005; http://www.indicare.org/tiki-read_article.php?articleId=118

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 01/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=128

Creative Humbug? Bah the humbug, let's get creative!

By: Mia Garlick, Creative Commons, San Francisco, USA

Abstract: Creative Commons has been criticized recently, in particular by legal counsel for the Hungarian collecting society ARTISJUS in a recent article in INDICARE, for being unforthcoming about its purpose and misrepresenting both its mission and licenses. Creative Commons welcomes the debate about copyright issues and Creative Commons' role in working to facilitate the interests of creators and users of copyrighted works. This article seeks to clarify some misunderstandings and misrepresentations about what Creative Commons is about and about the Creative Commons' licenses.

Keywords: opinion – collective rights management, copyright law, Creative Commons, creators

Introduction

Far from being humbug, Creative Commons (cf. sources) is a non-profit organization that has offices in San Francisco, London & Berlin and project leads around the world. Since 2002, Creative Commons has made available, for free, a range of licenses and tools for creators to make their works more readily available on terms that clearly signal what others may do with their works. In addition, Creative Commons' technology enables the development of search engines, similar to the Creative Commons-specific search engine now included as part of Yahoo!'s advanced search (cf. sources), that permits users to search for, and find, Creative Commons-licensed content according to its license terms.

With over 17 million linkbacks to Creative Commons licenses – or 1 out of every 530 webpages (based on Yahoo!'s index) now licensed under a Creative Commons license; with the Creative Commons licenses "ported" to 21 different jurisdictions and another 12 jurisdictions actively in the process of porting, Creative Commons is an established presence that clearly speaks to the needs and desires of many people who create copyright protected works.

On 24 June 2005, *Dr. Péter Benjamin Tóth* published an article that appeared in the INDICARE Monitor entitled "Creative Humbug" (2005). In it, Dr. Tóth expressed his discomfort with the "fishy smell" that surrounds Creative Commons. Dr. Tóth is, among other things, legal counsel for the Hungarian musical collecting society ARTISJUS.

Creative Commons appreciates the comments and concerns expressed by Dr. Tóth and welcomes this opportunity to clear the air, so to speak, and to dispel any concern of Dr. Tóth's, his colleagues or of any INDICARE readers that Creative Commons engages in a "whispering campaign" or a campaign of suggestions.

Creative Commons & ARTISJUS work toward similar goals

In his article, Dr. Tóth sets up an apparent opposition between the Creative Commons licensing model and collective management systems. Any such opposition is non-existent, or at least should be. Creative Commons and collective management organizations work towards similar goals – namely, representation of artists' interests and education about copyright issues.

It is useful to have the comments of Dr. Tóth given his position as legal counsel for ARTISJUS and given the role of ARTISJUS as a representative of Hungarian author's rights in musical and literary works as well as the rights of foreign rightsholders of public performance, mechanical reproduction and similar rights.

Creative Commons also works to serve the interests and needs of creators. Creative Commons is an enabler for creators to license their works and publish them more readily, for example, using our ccPublisher tool (cf. sources). Perhaps for similar rea-

sons, ARTISJUS implemented an "arrangement under which members can provide royalty-free access to their works through personal homepages or a free online storage space made available by ARTISJUS" (cf. sources).

Given ARTISJUS is working towards the same goals and representing, potentially, the very same individuals as those who are likely to be Creative Commons license adopters, its comments assist Creative Commons and the general public in more fully understanding creators' concerns and, thus, enable Creative Commons to better serve those concerns and enable the general public to respect these concerns.

One of Creative Commons' objectives is to raise awareness of copyright issues, and in particular, how they affect individual artists and creators, as well as users. By opening up this discussion, both Dr. Tóth, ARTISJUS and Creative Commons can continue to educate creators and the general public about copyright law and, hopefully thereby, promote the dual purposes of copyright law, as expressed in the Hungarian Copyright Law: to "create and maintain an equilibrium between the interests of authors and other rightsholders, as well as users and the public at large, taking into account the requirements of education, culture, scientific research and free access to information." (Hungarian Copyright Law (Act No. LXXVI. of 1999 on Copyright)).

Creative Commons' mission is clear & built on the flexibility inherent in copyright law but lacking in practice

Creative Commons' mission is clearly expressed on its home page as follows:

> "Creative Commons offers a flexible range of protections and freedoms for authors and artists. We have built *upon* the 'all rights reserved' of traditional copyright to create a voluntary 'some rights reserved' copyright. We're a nonprofit. All of our tools are free." (emphasis added)

As is clear from this statement, Creative Commons is based on the existing system of copyright. Creative Commons' approach of "some rights reserved" rather than being in opposition to the copyright law *per se*, is an alternative to two manifestations of copyright law in everyday life: (i) the default "all rights reserved" position that attaches to a copyrightable work the minute it is made, often without the creator's knowledge; (ii) the status quo "all rights reserved" model that serves as the standard business model for most copyright-based industries to date.

The minute you take the picture, hit the "save" button on your computer, record your song, or code your website, you are creating a copyright-protected work. Many people are unaware of this when they create copyright protected works as part of their daily lives or as part of their creative activity. Consequently, they do nothing about this, even if it does not accord with their preferences as to how others may use their work, and, thus, the default level of copyright protection that attaches to their work is "all rights reserved"– in other words, they, as the copyright owner, enjoy exclusive rights to control who may copy, adapt, distribute, transmit over the Internet, publish etc. (subject to some limited exceptions) their work by operation of copyright law, immediately upon having created a work that satisfies copyright law's requirements.

An example that illustrates this issue is the moblogging that occurred during the recent, horrific attacks on London. Several people, who were in the tube tunnels during and immediately following the attacks, including a person called *Adam Stacey*, took photos, using their mobile phones, of the scene before their eyes. (cf. O'Neill 2005, Alfie's Discotastic Moblog) The minute those pictures were taken, the default "all rights reserved" level of copyright protection applied. However, in the case of Adam Stacey, he sent the image to his friend *Alfie Dennen* and told Alfie that the image was too important, that it had to get out there. Consequently, the image was posted to Alfie's Discotastic Moblog under a Creative Commons Attribution License. The Creative Commons Attribution License enables anyone to copy, redistribute and adapt the work provided attribution is given to the author. Because of this license, the image quickly appeared on Sky,

Associated Press and other news services and Adam, previously, just a "citizen journalist" became a nighttime news reporter.

Adam and Alfie were sufficiently aware of copyright laws to modify their initial "all rights reserved" position to a "some rights reserved" position. Creative Commons licenses gave them the ready tools to do this, without having to take the time & expense to consult a lawyer (by which time the newsworthiness of the image may have dissipated). No doubt, most other people who use their mobile camera phone are not as aware as Adam & Alfie about the copyright implications of taking a photo and/or similarly do not have access to a lawyer to draft up more reasonable license terms; consequently, without more, their creative works will be subject to the maximum copyright protection possible under applicable laws. Anyone who then comes across these works must either: assume they are subject to "all rights reserved" protection and cannot incorporate it into their website, documentary or book without first taking the time to track down the owner and asking for permission; or, if they are unaware of copyright laws, and do so, they become an unwitting infringer. This is the situation even if the creator would have been happy for them to use the work in this way.

The other way in which "all rights reserved" has become the default and standard copyright position is through established industry business models. In the recording and publishing industries, for example, record labels and publishing companies frequently take either a transfer of copyright ownership or an exclusive license of all rights from the individual creator. These companies in turn then make the music or books available – as you can see if you check out the imprint page of the books on your bookshelf or the CDs in your CD rack—with the statement "© 2005. All rights reserved."

Creative Commons licensing is different to this model. In the first place, under the Creative Commons licensing model, copyright ownership can stay with the creator. In the second place, the copyright notice that is conveyed to the public states "some rights reserved" and the Commons Deed (the human-readable code) sets out the key terms of which rights are reserved and which rights are not.

Thus, Dr. Tóth's initial observation that "the 'some rights reserved' concept is therefore not an alternative to, but rather the very nature of classical copyright" is, in some limited respects, accurate; the Creative Commons licensing model works *because it is based on copyright* and thus, obviously the copyright system enables authors to license some of their rights and not others. The problem is that under default copyright rules or a general silence about the copyright status of a work and established business models, the practical application of copyright laws has trended away from flexibility, in favor of "all rights reserved." This is the issue that Creative Commons seeks to address by educating people about copyright issues – for creators by enabling them to make a choice that suits their preferences and clearly signalling what use others may or may not make of their works; for users by causing people to stop, look & think when they see a Creative Commons "some rights reserved" button as to which rights are reserved and which are not.

Creative Commons license adoption

Although Creative Commons started only three years ago, currently according to the Yahoo! Creative Commons-specific search engine, as noted above, there are over 17 million linkbacks to Creative Commons licenses and these linkbacks are spread throughout the world. In addition, as also noted above, to date, Creative Commons licenses have been "ported" (that is linguistically and legally translated suitable to a particular jurisdiction) in 21 jurisdictions around the world including such countries as Japan, Finland, South Africa, Brazil, Spain, Australia, Canada and South Korea.

Against this background, Dr. Tóth states that "[l]et there be no mistake: the CC licenses may be adapted to many jurisdictions, but they are not adopted *in* any jurisdiction…The state is not in a position to adapt and enforce the use of these uniform licenses." (emphasis in original)

This argument seems to be confused and is, thus, not a valid criticism. Two points may clarify the confusion. Firstly, Creative Commons is not representing, and neither does *The Register* article cited by Dr. Tóth in connection with his assertion (cf. Emert 2005), that a state has adapted or enforced a Creative Commons license. The adaptation work is carried out by Creative Commons project leads in each jurisdiction. For example, in Hungary, *Balázs Bodó* of the BUTE Center for Media Research and Education, *Attila Kelènyi* of Kiskapu Publishing, *Dr. Ágnes Dudás* from the FSF.hu Foundation for Promoting and Localizing Free Software in Hungary and *Dr. Anikó Gyenge* from the Legal Center for Infocommunication Issues at the Hungarian Academy of Sciences are carrying out this adaptation work. By way of further example, in Germany (the country cited in *The Register* article), Creative Commons worked with Professor *Dr. Thomas Dreier*, *Ellen Euler*, and *Oliver Meyer* at The Insitute for Information Law at the University of Karlsruhe and Institut für Rechtsfragen der Freien und Open Source Software (ifrOSS) to adapt the licenses for Germany.

Secondly, contrary to Dr. Tóth's assertion, Creative Commons licenses *have been adopted* by individual creators in numerous jurisdictions around the world. For example, recent statistics indicate that over 440,000 licenses have been adopted in Germany. In Spain, over 785,100 licenses have been adopted. In total, as noted above, 17 million licenses have been adopted and applied to online works.

Creative Commons is in talks with around 70 countries around the world and thus, we and our international Commons community are working to continue expanding global license adoption in each country that "ports" Creative Commons licenses.

Understanding the Commons Deed & the Legal Code

Creative Commons licenses are expressed in three different formats: the Legal Code (lawyer-readable), the Commons Deed (human-readable) and metadata (machine readable). The Commons Deed – being designed for the general public to read & understand – merely summarizes the key components of the Legal Code to render them effective for the average, legally untrained user; it clearly explains what, essentially, a user can and cannot do with the work.

Dr. Tóth is correct that much of what is in the Legal Code is not in the Commons Deed (or the metadata) and no doubt, all legally untrained people who use the Creative Commons licenses and/or works licensed under a Creative Commons license are thankful for this. For example, neither the "Warranties, Representations & Disclaimer" clause, nor the "Limitation on Liability" clause, nor the "Severability" clause nor the "No Waiver" clause are included in the Commons Deed or the metadata. These clauses – whilst necessary to construct a legal document – do & arguably should (for the sanity of the general public) remain the preserve of lawyers and the courts to argue about and interpret. When I buy a hair-dryer or park at the parking station, I am told that there are terms, have the opportunity to review them at my leisure, and am told the key terms. Similarly, the Creative Commons Commons Deed links through to the Legal Code and people have the opportunity to review the finer points of the legal drafting, if they chose, or to simply read the key terms as expressed in the Commons Deed.

The point of Creative Commons' three different expressions of its licenses is to facilitate greater use of copyrighted works, educate people about respect for copyright and how to comply with copyright laws and the Creative Commons licenses. The purpose of the licenses is not to educate every person to appreciate the finer points of legal contract drafting.

One unfortunate obfuscation made in Dr. Tóth's article is his assertion that

> "CC licenses are even more extortionary than an exclusive 'buy-out' contract from a global media company, where the author at least gets some money, and according to the legal regulations can revoke the license in some circumstances. To bring another example, a collecting society is obligated to give the possibility to its

> authors to 'take back' their rights if they are not content with the workings of the society."

Here, Dr. Tóth makes an inaccurate comparison between the Creative Commons licensing model and the model of many European collecting societies and so-called "global media company[ies]". The Creative Commons licensing model applies to an individual work at the creator's option. It does not apply to all present and future works of the creator. Many European collecting societies require creators to *transfer ownership* (not even just license) of certain righs in each and every one of their present and future works to the society. Moreover, many established content companies often require ownership of or exclusive rights in present work as well as ownership of or, at least options in, future works created by an artist. Creative Commons licenses are designed to enable the artist to retain ownership of their work and make decisions about how they want to license that particular work. Applying a Creative Commons license to one work does not require application of a Creative Commons license to any other work. In this way, therefore, it is possible for a creator to experiment with the Creative Commons licensing model. One clear example of this was the WIRED CD: Rip. Sample. Mash. Share. which contained tracks from 16 different artists including the *Beastie Boys*, *Chuck D*, *Gilberto Gil*, *Thievery Corporation*, *Zap Mama* and *David Byrne* all released under one of the Creative Commons Sampling licenses. (cf. sources) By releasing one track under a Creative Commons license, these artists did not thereby become bound to release any of their previous or future tracks under a Creative Commons license.

Moreover, applying a Creative Commons license to a particular work does not "lock down" that particular work to Creative Commons licensing exclusive of any other form of licensing with respect to that work. Creative Commons licenses are "non-exclusive"; thus, an artist can enter into different licenses, including revenue-generating licenses, in relation to a Creative Commons licensed work.

The history of Creative Commons license adoption to date demonstrates that there are three main ways in which an artist can earn income in connection with Creative Commons licenses.

Firstly, Creative Commons licenses can be applied to a work in a particular format to encourage awareness of the work and, thus, sales of the work in a different format. One example of this occurs in the publishing industry when authors and/or publishers release a book online under a Creative Commons license whilst selling hardcopies of the book.

One notable example is (unsurprisingly) Creative Commons' Chairman & CEO *Lawrence Lessig* who released his book "Free Culture" under a Creative Commons Attribution-NonCommercial license. (cf. sources) The book is now in its third print run.

Another example is *Kembrew McLeod*'s book "Freedom of Expression®", which was also released online in PDF format under a Creative Commons Attribution license and sold in hardcopy format. (cf. sources) By making it freely available online, Kembrew's book was able to circulate well beyond its hardcopy distribution in the United States and Japan, receiving responses and conference speaking invitations from people who shared research interests in various European, Asian, and African countries. In addition, the publicity surrounding his online Creative Commons release of the book generated hardcopy sales through Amazon.com.

A further example in the publishing arena is the open access law publishing program, recently launched as part of Creative Commons' Science Commons publishing project. (cf. sources) The publishing model adopted by the program and signed on to by, to date, 23 prominent US, English & Canadian law journals, enables the author to: retain their copyright in their paper and grant the publisher a limited-term, exclusive license for commercial publication whilst also making the paper available to the public under a, for example, Creative Commons Attribution-NonCommercial-NoDerivatives license. In this way, the commercial publishing model of the journals is not disturbed but authors

and the general public from the greater availability of the author's writings.

In the music world, Magnatune is an innovative Internet record label that started in 2002. (cf. sources) Magnatune releases streams and downloads of its artists under a Creative Commons Attribution-NonCommercial Share-Alike license but sells their albums on CDs.

Secondly, a Creative Commons license can be applied to a work to signal to the general public the terms on which they may use the work and then interested parties may enter into a commercial side-deal in relation to the work. By reason of the Creative Commons' metadata and Creative Commons-specific search engines such as that now incorporated in Yahoo!'s search engine, Creative Commons licensed work can be more readily located by persons interested in making commercial uses of their work.

Thus, by licensing content within the Creative Commons network, access to a person's creativity can be substantially increased. Business 2.0, for example, reported on the story of a Slovakian artist who used Creative Commons licenses to make his music available. That then translated into two commercial contracts with U.S. companies to use his music in their projects (cf. Raskin 2004).

Thirdly, Creative Commons licensed works can advertise a creator's talents and secure them a commercial arrangement for different or future works. One such example is that of "*MinusKelvin*", a physics and calculus teacher by day, a composer by night. (cf. MinusKelvin 2005) He makes tracks available to podcasters using Creative Commons licenses and recently joined the ccMixter site. ccMixter is a site created by Creative Commons that enables people to post their music to the site under Creative Commons licenses that permit remixing. People can then remix the tracks and upload their remixes. Runoff Records, Inc. signed MinusKelvin after discovering him on ccMixter. Together with another ccMixter musician, *Pat Chilla*, MinusKelvin will now be doing the music for the next three seasons of America's Next Top Model.

Thus, Dr. Tóth asks "[w]hy should anyone invest in works that are already widely available for free?" The response to that question, as the above examples illustrate, is that the reasons are multiple. Digital technologies make it easier, cheaper & quicker than in the analogue world for individual consumers to become a producer of high-quality material; so professional, indeed, that there have been reports of photograph printing services refusing to print personal photos of members of the general public for fear that they are the work of professional photographers and even, in some instances refusing to release people's personal happy snaps back to them without a signed copyright release. (cf. Seltzer 2005) Just as digital technologies make us all professional creators, so too do they enable people to advertise their works and/or their talent, share their creativity more easily and more readily, and clearly signal to members of the pubic that they welcome the use and reuse of their work.

Enforceability of Creative Commons licenses

Finally, license enforcement – a topic close to many lawyers' hearts! Dr. Tóth queries the practical enforceability of the Creative Commons licenses and suggests that the issue of enforcement is somehow more difficult under the Creative Commons licensing model, than under a collecting society or "all rights reserved" model.

This contention is without merit. The issue of knowing when a person has violated a license term applies equally in relation to a Creative Commons licensed work as much as it does to a work licensed under any other model. Once you sell a book or allow someone to download a track from a site, how do you know that they will use it consistent with the license terms and/or any technological restrictions? This is a challenge that all creators and organizations that assist them – such as Creative Commons and ARTISJUS – face. If artists and the organizations that assist them work together we can attempt to solve this problem by teaching people more about copyright law and why & how to respect.

In addition, Dr. Tóth claims that because the generic license originated in the United

States, the local licenses adapted to the jurisdictions of Germany, France, Spain, Japan etc. will not be sufficiently tailored to the local laws of those jurisdictions. Somehow, because CC-HQ has final approval over the final draft of the jurisdiction-specific licenses, the licenses will be invalid under local laws. Leaving to one side the obvious factual point of distinction, namely, that the actual location of the office that engages in final review of the licenses is in Berlin, Germany, Dr. Tóth is clearly insufficiently familiar with our license finalization process.

Everything about Creative Commons involves community involvement and community feedback. This is nowhere more apparent than in the international community, especially given the expertise that exists within the international Creative Commons-minded community. The license "porting" process involves our local project lead preparing the first draft of the license, linguistically and legally adapted for the specific jurisdiction, this draft is then circulated on an e-mail discussion list of interested participants in that jurisdiction. These list participants debate the various aspects of the license, in particular as it pertains to their jurisdiction. These comments are then incorporated into a further draft, which is again submitted for community review. A final draft is then prepared and CC-HQ's Berlin office confirms license interoperability and otherwise assists with drafting issues that may have arisen on the country discussion list. The role of CC-HQ's Berlin office is simply one of assistance and facilitation. At all times, substantive review and amendment of the licenses to comport to local legal requirements is undertaken by experts in that jurisdiction.

No doubt, the Creative Commons license will one day be tested in a court of law, similar to the recent case before a Munich court involving the GNU-GPL license (cf. Shankland) and, when that situation occurs, we will all observe the enforceability of the license for the particular dispute in question. Until this day, however, and most likely even after this day, there is no basis upon which to claim that Creative Commons licenses are unenforceable. Every member of our community is working to ensure that they are locally enforceable in anticipation of when a court date is set, and also, that the licenses properly represent and respond to the needs of artists.

For Dr. Tóth to imply that because Creative Commons does not provide legal advice and enforcement assistance, Creative Commons "simply shrug[s] their shoulders" when it comes to helping people enforce their rights, flies in the face of reality. We receive countless queries and requests for assistance and, to the extent we are able to locate a suitable volunteer legal service in the inquirer's jurisdiction, we direct them to that service. Indeed, to the extent that ARTISJUS provides pro bono legal assistance to artists, Creative Commons looks forward to working with ARTISJUS in this regard.

Bottom line

Creative Commons welcomes the debate and feedback about our licenses. Creative Commons constantly strives to develop licenses and tools that are adapted to and serve the needs of creators and users of copyright works. Because the Creative Commons licensing model is different to the established business models and the default "all rights reserved" copyright model that has existed in practice historically, Creative Commons often engenders debate, concern and, sometime, confusion as to what Creative Commons does and how its licenses and tools operate. Thus, Creative Commons appreciates the opportunity to try to clarify these issues but, more importantly, the opportunity to generate discussion of these issues. Particularly, in the case of ARTISJUS and its fellow collecting societies, a common ground exists on which to explore these issues because all organizations serve similar interest groups.

Ultimately, however, such discussion serves an incredibly useful purpose of holding up the mirror and enabling us all to consider and opine on how we can all work towards making copyright law better fulfil its objectives.

Sources

- Alfie's Discotastic Moblog: http://moblog.co.uk/view.php?id=77571
- ARTISJUS: There from the start, International Confederation of Societies of Authors & Composers http://www.cisac.org/web%5Ccontent.nsf/Builder?ReadForm&Page=Article&Lang=EN&Alias=CN-2004-01-ARTISJUS
- ccMixter: http://ccmixter.org/
- ccPublisher: http://creativecommons.org/tools/ccpublisher
- Creative Commons website: http://creativecommons.org
- Creative Commons' internationalization project: http://creativecommons.org/worldwide/
- Emert, Monika: Germany debuts Creative Commons. TheRegister, June 15, 2004 (*available at:* http://www.theregister.co.uk/2004/06/15/german_creative_commons/) (last accessed July 19, 2005)
- Lessig, Larry: Free Culture, http://www.free-culture.cc/
- Magnatune: http://www.magnatune.com/
- McLeod, Kembrew: Freedom of expression®, http://kembrew.com/books/index.html
- Minus Kelvin: http://www.lessig.org/blog/archives/002890.shtml
- O'Neill, Rob: Now we're all journalists. The Age, July 11, 2005, http://www.theage.com.au/news/creative--media/now-were-all-journalists/2005/07/10/1120934123353.html?oneclick=true (last accessed July 19, 2005)
- Raskin, Andy: Giving it away for fun & for profit. Business 2.0, April 20, 2004, http://www.business2.com/b2/web/articles/0,17863,608619,00.html (last accessed July 19, 2005).
- Science Commons Open Access Law Program: http://sciencecommons.org/literature/oalaw
- Seltzer, Wendy: A photofinish for copyright's unintended consequences; posted to Corante: Copyfight, June 7, 2005, http://www.corante.com/copyfight/archives/2005/06/07/a_photofinish_for_copyrights_unintended_consequences.php (last accessed July 19, 2005); *see also,* Balint, Kathryn, 'Snap Judgments', San Diego Union-Tribune, May 30, 2005, http://www.signonsandiego.com/news/computing/personaltech/20050530-9999-mz1b30snap.html (last accessed July 19, 2005).
- Shankland, Stephen: GPL gains clout in German case. CNet News.com, April 22, 2004, http://news.com.com/GPL+gains+clout+in+German+legal+case/2100-7344_3-5198117.html (last accessed July 19, 2005)
- Wired CD: http://creativecommons.org/wired/
- Yahoo! Advanced Search: http://search.yahoo.com/search/options?fr=fp-top&p=
- Tóth, Péter Benjamin: Creative Humbug. Personal feelings about the Creative Commons licenses. INDICARE Monitor, Vol. 2 No 4, June 2005; http://www.indicare.org/tiki-read_article.php?articleId=118

Acknowledgement: This article was prepared with the invaluable assistance of Attila Kelènyi attila@kiskapu.hu, part of the Creative Commons Hungary team, and builds on the comments submitted by Balázs Bodó bodo@axelero.hu, also part of the Creative Commons Hungary team, directly in response to Peter Benjamin Tóth's article (cf. http://www.indicare.org/tiki-read_article.php?articleId=118#comments).

About the author: *Mia Garlick* is the General Counsel of Creative Commons Corporation. Before joining Creative Commons, Mia worked for several years in private practice as an intellectual property attorney in Sydney, Australia, and Silicon Valley, US. She can be contacted via e-mail at: mia@creativecommons.org.

Status: first posted 27/07/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=124

A breakdown of consumer protection law in the light of digital products

By: Martien Schaub, Mitopics, Gouda, Netherlands

Abstract: Consumers using digital content will often find themselves confronted with DRM. Some consumers have attempted, with little success, to argue that these measures interfere with their "right to a private copy", referring to the exception made with regard to this in copyright law (Helberger 2004). Another area of law that can be drawn into this is consumer law. Consumer law contains several legal instruments that protect the consumer who is considered to be the weaker party in relation to a commercial party.

Keywords: legal analysis – consumer law, consumer expectations, consumer rights, fair dealing, transparency – EU, United Kingdom, The Netherlands

Introduction

In the first INDICARE Monitor of this year *Rüdiger Grimm* (2005) remarked: "virtual goods are made for purchase and usage". When using digital products, consumers will find that some uses are not possible as a result of DRM. DRMs are used to protect the interests of the distributors and artists; however at some level this will interfere with the interests of the consumer who expects that he can make certain uses of the content he obtained. This contribution discusses several legal instruments that might come to the aid of the consumer in relation to the consumption of digital goods (for an overview of European consumer protection law see De Witte 2004).

Preliminary question: are digital products goods or services?

In law it is important to establish if you are dealing with either goods or services, because in some cases there are different rules for the one and the other. The definition of "good" generally relates to physical appearance of something, while service provision concerns the performance of some sort of act other than the delivery of a good.

Digital content consists of bits and bites that are normally connected to a physical carrier such as a CD or a hard drive. If digital content is connected to a carrier, selling it can be characterised as the selling of a good, because a tangible changes hands. A digital delivery (for example via internet) merely consists of the transfer of bits and bytes. In that case, it becomes problematic to characterise such a delivery as the delivery of a good. In the past this topic has been addressed in relation to electricity (HR 23-3-1921) and computer data (Hof Arnhem, 27-10-1983). In case law these have been considered to be equal to a good, which can be stolen. However, this conclusion was drawn in relation to criminal proceedings. These solutions however cannot simply be transposed to private law issues.

In the discussion concerning the legal distinction between goods and services it is important that the context and the purpose of the rules of law are taken into account. In the context of consumer law, it seems unfair to treat a song differently, depending on the manner it is formatted or delivered. If consumer rights are dependent on the manner of distribution, this opens the possibility for distributors to choose the manner that favours their position. For practical purposes, it can therefore be preferable to consider the delivery of a digital product to be equal to the delivery of a good. Reference can be made to the analogy with sale of books and CDs, which are generally considered to be sale of goods, regardless of the fact that what is actually sold is copyrighted material. The discussion of rights and duties below will assume that the rules of sale of goods can apply to the selling of digital content, either because the product can be qualified as a good or, if this fails, by analogy.

Contract law

Non-compliance

In general, contract law requires that the seller should perform in conformity with the contract. English law in this respect requires that the goods supplied should be of satisfactory quality and specifies that this requirement is met if the sold good is as fit for the purpose for which goods of that kind are commonly bought or as it is reasonable to expect having regard to any description applied to them, the price (if relevant) and all other relevant circumstances. An exception applies when the buyer's attention was specifically drawn to the "defects".

Dutch law requires that a seller should deliver in conformity with the contract and specifies that this is the case if the good has the characteristics which are necessary for a normal use to be made of it and whose presence he did not have to doubt, as well as all the characteristics which are necessary for a special use which has been mentioned in the contract (for a comparison of Dutch law, English law and French law on this topic see Girot 2001).

A similar rule has been laid down in the European directive on sale of consumer goods (Directive 1999/44/EC). This directive states that goods are presumed to be in conformity with the contract:

- if they correspond to the description given by the seller or to a sample or model shown to the consumer,
- if the goods are suitable for the special use indicated in the contract,
- if they are fit for the purposes for which goods of the same type are normally used,
- if they show the quality and performance which are normal in goods of the same type and which the consumer can reasonably expect, given the nature of the goods and taking into account any public statements by the seller the producer or his representative.

Relevant factors to determine if there is breach of contract (either in England or in the Netherlands) can be the nature of the product sold, the knowledge the seller has about the intended use, price, the state of the market and reasonable expectations of the consumer.

Applying the legal norms to digital content equipped with DRM-techniques entails that it has to be established what can be considered "normal use" of digital content, what digital content is "commonly" bought for and what is reasonable to expect.

Unfair contract terms

Basing a claim on breach of contract is rendered difficult if the use of the DRM-techniques is accompanied by (pre-contractual) warnings by the supplier. In that case the consumer has fewer possibilities to argue that expectations were not met. However, this does not affect the possibility to base a claim on unfair contract terms. In this context one can think of the Unfair Contract Terms Act in England, and the rules regarding general terms in Dutch law, which include a black list of terms that are considered to be unreasonably onerous and a grey list of terms which are suspected to be unreasonably onerous. In both countries it is up to judges to further determine in the context of each particular case if certain terms are unfair or unreasonably onerous.

On European level there is the unfair contract terms directive (Directive 93/13/EEC) harmonising the laws of the member states with regard to this issue. According to this directive terms are unfair if, contrary to the requirement of good faith, they cause a significant imbalance in parties' rights and obligations arising under the contract, unless the terms were individually negotiated.

Relevant in the assessment is the nature of the goods or services, and all other circumstances. Circumstances could be the price and the reasonable expectations of the buyer. Again, reasonable expectations turn up, as well as good faith and circumstances of the case. How does this translate to the supply of digital content with DRM? Opinions of what is "reasonable" can vary.

Unfair commercial practices

Related to the rules concerning contract law are the rules concerning unfair commercial practices. The laws of the member states will be harmonised on this point after the imple-

mentation of the recently adopted directive on unfair commercial practices (Directive 2005/29/EC). The directive protects the consumers' economic interests against unfair practices that take place before, during or after a commercial transaction. The directive does not prescribe what is considered to be "fair", but instead indicates which practices are considered to be unfair:

- if it is contrary to the requirements of professional diligence,
- if it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed.

Professional diligence is defined as the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity. An important factor in the determination if a certain practice is unfair is the amount and type of information that is provided to the consumer.

These open norms such as "good faith" and "reasonable expectations" make for flexible legal norms that can be applied to numerous situations. The downside is that little legal certainty is offered and the decision will depend on circumstances of the case.

Defective products

The European directive on product liability protects against material damages afflicted to persons (death and personal injury) and damage to property (Directive 85/374/EEC). Apart from the protection measures that are so aggressive that they will harm the consumers' computer, the DRM-techniques will commonly not cause material or personal damage.

According to the directive a product is defective if it does not provide the safety, which a person is entitled to expect, taking all circumstances into account, including:

- the presentation of the product;
- the use to which it could reasonably be expected that the product would be put;
- the time when the product was put into circulation.

Although many consumers may currently expect that some sort of DRM is connected to digital content, it is less likely that they will expect that such measures will cause damage, such as harm the hard-drive of a PC. Even if this is clearly communicated towards the consumer that damage might occur, it can be argued that a DRM-techniques should not harm the consumers' computer. Although probably effective in protecting intellectual property rights, it can be argued that this does not pass the proportionality test: the punishment is far too grave in relation to the "crime" committed.

Besides the specific regime concerning defective products, consumers may rely on general liability rules such as tort of negligence in England or *onrechtmatige daad* in the Netherlands. Roughly speaking, general liability rules require that adequate duty of care is observed concerning the interests of others.

Transparency

In the previous paragraphs several references can be found to the presentation of the product, information provision and pre-contractual warnings. This relates to transparency: information with regard to the product and the contract terms is relevant in the determination of the lawfulness of the distribution of the product. The law also contains several explicit information duties that need to be fulfilled by the seller. The distant selling directive (Directive 97/7/EC) imposes pre-contractual and post contractual information duties which include amongst others the obligation to communicate the main characteristics of the goods or the services (note that no distinction is made between goods and services). Furthermore the e-commerce directive (Directive 2000/31/EC) requires that the price is clearly indicated and that the contract terms and general terms are presented in such a manner that they can be stored and reproduced.

These information requirements can assure that consumers know what they can expect, and prevent that consumers are disappointed

or misled. However this cannot remedy the situation where the suppliers of digital content make use of contract terms unfavourable to the consumer, they merely oblige the suppliers to communicate these terms clearly to the consumer (compare Guibault and Helberger 2005).

Bottom line

Above discussed rules show that consumer expectations play a crucial role in the determination if a certain product or a contract relating to it is lawful. Related to this is the generally accepted practice in a certain domain. As the domain of digital content delivery is relatively new, it is hard to determine what is generally accepted in the domain and what consumers may or may not expect. The fact that a diversity of digital products combined with different manners of distribution are becoming available complicates the issue.

What an average consumer can expect today when he buys digital content is a right to use the content, which is subjected to more or fewer limitations. Whether these limitations are legitimate cannot be determined solely with the legal standards offered by consumer law. These legal standards contain open norms, which do not provide for a conclusive answer. The best instrument that is offered to the consumer appears to be the information duties of the seller. In case of lacking, inadequate or false information about the product, a consumer may successfully base a claim on breach of contract or unfair practices.

Although the information duties cannot remedy that sellers use unfavourable terms, clear information allows the consumers (or consumer organisations) to determine their positions and possibly take action concerning the acceptability of the digital products and the terms under which they are marketed. Tools to do so are handed to these players by the law.

Sources

- Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the member states concerning liability for defective products, OJ L 210, 7-8-1985
- Directive 93/13/EEC on unfair terms in consumer contracts, OJ L 95, 21-4-1993
- Directive 97/7/EC on the protection of consumers in respect of distance contracts, OJ L 144, 4-6-1997
- Directive1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees, OJ L 171, 7-7-1999
- Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17-7-2000
- Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market, OJ L 149, 11-6-2005
- Girot, C. (2001): User Protection in IT-contracts. Den Haag: Kluwer Law International 2001
- Grimm, R. (2005): Where do DRM- and e-payment systems meet? INDICARE Monitor vol. 2, no 1 25 March 2005; http://www.indicare.org/tiki-read_article.php?articleId=86
- Helberger, N. (2004): It's not a right silly! The private copying exception in practice. INDICARE Monitor vol. 1, no. 5, 29 October 2004; http://www.indicare.org/tiki-read_article.php?articleId=48
- Hof Arnhem, 27-10-1983, NJ 1984, 80 (Computerdata)
- HR 23-3-1921, NJ 1921, p. 564 (Electriciteitsarrest)
- de Witte, M., Vermeersch, A. (2004): Europees consumentenrecht, Apeldoorn: Maklu 2004
- Guibault, M., Helberger, N. (2005): Copyright law and consumer protection. Report for the European Consumer Law Group, February 2005

About the author: *Martien Schaub* studied law in Nijmegen and wrote her Phd thesis at the faculty of technology and Management at the University of Twente. Currently, she is a legal ICT consultant. Contact: m.schaub@mitopics.nl.

Status: first posted 26/07/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=123

What Norwegian politicians should know about DRM

By: Christine Hafskjold, The Norwegian Board of Technology, Oslo, Norway

Abstract: The Norwegian Parliament has recently passed important amendments to the Norwegian Copyright Act. The process to this point has been long, and there have been many sidetracks, particularly related to the technologies affected by the act – such as Music CDs, copy protection and MP3 players. To help clear up some of the technical issues, The Norwegian Board of Technology published a newsletter on technological measures and DRM.

Keywords: policy analysis – consumer rights, copyright law, EUCD, fair use, technical protection measures – Norway

Norway's approach to the Infosoc directive

In February 2005, the Ministry of Culture and Church Affairs submitted its White Paper on amendments to the Norwegian Copyright Act. The media immediately picked up on the section dealing with the circumvention of technological measures and named the proposal "the MP3 Act". Media coverage circled round a narrow selection of topics:

- **Every 14-year old in the country will become a criminal!** (Because they will want to copy their CDs to their iPods.)
- **Meet the politicians who own an MP3 player and hear what they feel about the proposal!** (Because their opinion is more informed than that of the other politicians?)
- **We have surveyed the parliament and this is the MP/MP3-player ratio of the different parties!** (Parties where no MPs have MP3 players shouldn't get to vote on this matter at all?)

Need for information

The Norwegian Board of Technology (NBT) is an independent body for technology assessment established by the Norwegian Government in 1999, following an initiative by the Norwegian Parliament (Stortinget). The Board had already scheduled a project on DRM for the autumn of 2005. However, from the media coverage, and the open hearing held on the proposition, it was clear that more information was needed on technological measures and DRM.

Aided by experts in law and cryptology, The NBT set out to give the Members of Parliament some balanced information on what DRM is and how it can come to affect how we deal with digital content in the future. The hope was that by providing balanced and easily understandable information on this matter, the politicians would also get a chance to focus on the other important aspects of the proposition: How to ensure that intellectual property rights are not violated in the digital age.

This resulted in a four page newsletter called *Technological measures – DRM*. The newsletter addresses the challenges digital technology means for intellectual property, focusing on music and film in particular, as the confusion in regard to this seemed to be the biggest. Also copying and distribution of this type of content has become cheap and easy – and in large groups of the population – widely acceptable.

Why is DRM relevant to this?

The obvious benefit of DRM is the possibility of charging a different price for digital content depending on the need of the customer. The customer can choose to download a film for watching once, or she can choose to buy a piece of music to store and copy to any format she wants. Most people today have no problem accepting that when you *rent* a DVD, you only buy a limited right to view it. You cannot copy it for private use or sell it to someone else – that would require you to *buy* the DVD. Transferring this concept to music, films and books in digital form is the challenge.

Much of the focus so far has been on copy protection on CDs and DVDs, and the fact

that the new law will prohibit the circumvention of such measures. Copy protection can be seen as a primitive form of DRM, restricting the right to copy a CD. The problem is that the consumers don't see it this way – it looks like a regular CD and costs the same, so why are the rights limited? To make matters worse, quite a few of these CDs don't play in all types of CD-players, and making a copy can in most cases solve this problem. This led the Ministry to add an exception to the rule: You may circumvent a technological measure to be able to play your music on "relevant playback equipment". In the proposal from the Ministry, MP3 players were not considered relevant equipment for playing CDs, hence all the fuss in the media.

As "everybody" predicts that traditional copy protection will be replaced by DRM (or something similar) in the future, how DRM works and how it affects the protection of digital property rights is an extremely relevant issue when dealing with circumvention of technological measures. Limiting focus to the copy protection schemes we see today is clearly not sufficient.

Challenges with DRM

Limiting "fair use"?

In the proposal from the Ministry, circumventing technological measures is not legal when a contract for the use of the intellectual property has been made between the consumer and the property owner, and the property is purchased over the internet. As a DRM-system will contain such a contract, the deployment of DRM systems will mean that the regulation of consumer rights in this area is transferred from the authorities to the property rights owners: If no service that allows copying a piece of music or a film for private use exists, then the right to "fair use" will effectively disappear. In the newsletter to the Norwegian Parliament NBT recommends that the politicians watch the development closely, and take the appropriate measures to revise the law, should consumer rights be restricted as a result of this.

Hardware problems

Many consumers are concerned about DRM-systems that are linked to a specific hardware, and only allow the content to be played/read on this. Systems of this kind have made consumption of legally bought content difficult after a disc crash or after replacing an old PC. It's assumed that this type of problems will cause consumer reactions, and that alternative solutions will emerge.

Privacy issues

Privacy is an area where DRM has caused reason for concern. Several systems require the user to identify her self to access digital content. In this way, the supplier of the DRM system can get access to the user's media habits and in theory use this for promotion or in pricing. The NBT is of the opinion that it should still be possible to consume media content anonymously in the future.

Proprietary formats

Several DRM systems are in use today. The best known and most used are connected to Apple's iTunes and Microsoft's Windows Media Player. Both of these use proprietary formats that stop music or film from being played on a player of the consumer's choice. Some services in Norway today require that you have a specific media player to download content, i.e. Microsoft Windows Media Player.

If this type of connection between content and player becomes the norm, it can contribute to limiting the competition in the market for media players (hardware and software). It is recommended that The Norwegian Competition Authority should monitor developments closely.

From a consumer perspective, it's important to get global, open standards in place, to ensure that all media players can read the digital rights information and relate to this. The choice of media player will then be entirely up to the consumers. The authorities can stimulate this by demanding open standards in public services that use DRM.

When is circumvention of technological measures OK?

The cracking of technological measures to expose security issues has been much discussed. It's not unusual that research institutes and others identify security issues in software and then publish their findings.

After the Digital Millennium Copyright Act passed in the US, research institutes have expressed a reluctance to publish findings out of fear of prosecution. The EUCD has suggested that the protection of technical measures should not restrict the possibility to do research on cryptology, so as not to run into the same problem.

Proprietary DRM systems pose a problem for the developers of open source software (OSS). In order for this type of software to be able to read proprietary formats (like Microsoft Word), they must "reverse engineer" the format to find out how to read and present it. The proposal to protect technical protection systems means that doing the same thing to a DRM format will be illegal.

The purpose of circumvention in this case is not to get access to the content for free, but to get access to the rights information in order to treat the content in the same way as the intended media player would.

The NBT sees the OSS environment as an important competition corrective in a market dominated by big software development companies. It's therefore important that legislation in this area doesn't limit OSS developers' opportunity to deliver competitive solutions. Stimulating the development and use of open standards can be one way to go in this matter; another can be to open for an exception in the legislation similar to that of cryptology.

Bottom line

The Standing Committee on Family, Cultural Affairs and Government Administration gave its recommendations to Parliament on May 30th, and the act passed on June 4th. The consumer perspective got a broad place in the debate, and the outcome can also be perceived as consumer friendly, as it leaves an opening for circumventing technical measures to copy music from CDs to MP3-players (for private use). This means that the committee goes a lot further than the Ministry, that clearly stated that MP3 players should not be considered "relevant playback equipment. The committee explicitly states that the right to make private copies ("fair use") shall exist also in the future. It also states that DRM-systems will be important to uphold intellectual property rights in the future, but that such systems should not violate privacy or consumer rights. It also states that shifts in the competition in the market for playback equipment should be watched and handled by The Norwegian Competition Authority. Even though the committee's recommendations regarding privacy, consumer rights and competition are general, and it's unclear how they will be upheld, it's gratifying that these issues were in fact addressed. Only the future can show how it all will work in practice.

Sources

- Teknologirådet. Nyhetsbrev nr 9, april 2005 (in Norwegian): http://www.teknologiradet.no/files/tek_nyhetsbrev_nr_9_copy4.pdf
- White Paper from the Norwegian Ministry of Culture and Church Affairs (in Norwegian): http://odin.dep.no/filarkiv/237235/OTP0405046-TS.pdf

About the author: *Christine Hafskjold* works as a project manager with The Norwegian Board of Technology. Her main focus is projects related to ICTs, such as *Software policy*, *ICTs and privacy*, and *eGovernment*. Previous to her engagement with the NBT, Hafskjold has 10 years experience in IT consulting, both as a Project Manager and Systems Architect.

Status: first posted 18/07/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=121

Podcasting-profit-possibilities. Will DRM invade the scene?

By: Nicole Dufft, Berlecon Research, Berlin Germany

Abstract: Podcasting is one of the latest hypes in media publishing. Podcasts were originally produced and published for free by private radio aficionados. But with the growing popularity of this new media format, podcasts are increasingly becoming of interest to commercial media companies. A number of yet unresolved copyright and licensing issues are, however, limiting the potential of this digital format. This article takes a look at these issues, at potential business models and at the possible future role of DRM.

Keywords: economic analysis – business models, digital broadcasting, DRMS, licensing contracts, podcasting

Introduction

"On-demand" is a concept that is now also available for radio: Podcasts are radio programs in digital audio format (MP3, AAC) that can be downloaded from the Internet and synchronised with any MP3 player (not only with Apple's iPod as the name would suggest). They are distributed via the Internet exclusively, in contrast to traditional broadcasts. What makes this new concept of radio programs very appealing is that podcasts can be subscribed to over RSS-feeds (Rich Site Syndication, an XML-based summary of a webpage). This means that each new radio show is automatically downloaded to the PC and synchronized with the portable player and can be consumed whenever and wherever you want.

The production of a podcast is almost as easy as subscribing to it and requires not much more than a PC and a microphone. Many podcasts are, therefore, produced by amateur broadcasters and cover everything one can imagine from weekly reviews of books or movies, over daily English lessons, to morning and evening prayers ("Praystation Portable", "Godcast"). Podcasts are the audio equivalent to weblogs and are – as weblogs – a tool for narrowcasting as opposed to broadcasting (narrowcasting is the use of media to reach a specific audience).

The popularity of podcasts has lately been boosted by Apple's new iTunes version 4.9, which now supports podcasts. (While there are also videocasts, they are not the focus of this article.)

First steps from niche to mainstream?

A growing number of public and private broadcasters, e.g. BBC, Disney or Newsweek, as well as a variety of companies are experimenting with the new medium. So far, most podcasts are freely available on the Internet and do not contain commercials or advertisements. This could change, however, with the growing popularity of podcasts. The research company Forrester expects that by 2010 12.3 million US households will listen to podcasts (Forrester Research 2005).

Apple's support of podcasts in its latest version of the iTunes software can be regarded as a first step from niche to mainstream. Within the first two days after release, iTunes-clients subscribed to more than one million podcasts. iTunes allows customers to search for podcasts in a directory of more than 3,000 shows and to easily subscribe and synchronize them.

Copyright licensing schemes need to catch up with podcasting technology

The main factor that is currently limiting the potential uptake of podcasting is copyright. Most podcasts are limited to talk-radio today, because copyright legislation and existing licensing schemes do not appropriately cover music podcasts. "Indeed, copyright law has yet to catch up with the technology of podcasting" (Didden 2005).

The problem is that a music podcast does not only involve the public performance and broadcast of musical works, it also involves the playing and possibly the reproduction of a sound recording, since podcasts are

downloads and single songs could be extracted from them. While public performances of works are handled by the performance rights organisations like GEMA in Germany, PRS in the UK or SACEM in France, artists or their labels have the right over sound recordings. Playing music in a podcast, therefore, requires the approval of a collecting society as well as of the artist or its label. However, neither the collecting societies, nor the major record labels have developed common licensing schemes for podcasting yet.

While in the US, the collecting societies ASCAP and BMI have claimed the rights to performance royalties arising from podcasts, the German GEMA, for example has no concept for podcasting until now (Sixtus 2005).

Some artists and small record labels explicitly allow the use of their works in a podcast. Creative Commons (CC) offers an audio license that covers the use of musical works in non-commercial podcasts. The open music record label Magnatune, for example, licenses albums with a CC license for podcasts. Customers that want to buy the music can pick the price, starting at $5 (Buckman 2005).

Podcasts that feature music without the approval of artists or labels risk being sued by the music industry. So far, podcasting hasn't been popular enough to interest lawyers but this could well change soon.

New Business models for podcasts?

Copyright issues might become especially relevant if podcasting moves from home-made, not-for-profit, to commercial. With podcasting gaining so much popularity, we can expect that podcasts will be commercialized. Possibilities to make profit with podcasting are podcasts as a marketing tool, sponsoring and advertisements, or paid subscriptions.

One of the first companies that wants to help podcasters make money is BoKu Communications, founded by one of the inventors of podcasting, *Adam Curry*. BoKu produces successful podcasts and sees itself as a leader in commercializing the podcast movement through marketing, advertising, commerce and other vehicles. BoKu claims that "Podcasting is the ultimate narrowcast environment. Podcast listeners are early adopters. Podcast producers are early influencers." which makes podcasts an ideal tool for marketers. Podcast listeners represent an attractive demographic of early adopters that are young and technically savvy (Rubel 2004) and podcasts often target a very narrowly defined interest group.

Marketing

Podcasts are already used as a tool for marketing and to improve customer relationship. Large broadcasters such as BBC or ABC news surely have their customers in mind when offering own podcasts. Another example is Virgin Atlantic that offers podcast-travel guides as a customer-relationship-tool. In the US, politicians like *John Edwards* and *Arnold Schwarzenegger* have been using podcasts during election campaigns.

But podcasts can also be used to promote content, especially music. They are a promising way for unknown musicians to gain exposure. The BMI, for example, is offering its own podcast "See it Hear First" to promote newcomer artists. In another case, a Scottish music fan used his podcast to expose the world to tartan rock (BBC News). Podcasts can provide more information about the artist and direct interested listeners to an online music store, where the featured tracks can be purchased. For music labels podcasts could become another viable distribution channel – on the condition that licensing problems can be solved (see below).

Sponsoring / Advertisements

Podcasts can also be used for advertisement by inserting audio spots in the podcasts. This, however, diminishes the attractiveness of podcasts to their users, since commercial-free radio shows are seen as a major advantage of podcasting over traditional broadcasting.

Another possibility is sponsorship, where companies underwrite an entire podcast. Condom manufacturer Durex, for example, became one of the medium's first advertisers paying for product placement on the "Dawn and Drew Show", a very popular podcast where a couple talks about their private sex life. The ads are not typical radio "spots" –

Durex is paying the show's producers to talk about the condoms as part of the show's content.

Paid subscriptions

While so far most podcasts are offered for free, very popular shows and premium content could charge subscription fees in the future. However, one has to keep in mind that few media giants have been able to sell enough subscriptions to their web-based content to be anywhere close to profitable (Knowledge@Wharton 2005).

In addition, when podcasts are offered for money, the question arises, how the illegitimate distribution of these audio files could be prevented – and here the question of copy-protection and DRM comes into play.

DRM-protected podcasts?

DRM and copy-protection could become relevant for podcasting in two respects: First, if a business model for paid podcasts should emerge, the distribution of the audio files needs to be controlled. Second, if podcasts are to feature music, DRM-issues arise. Generally, many labels will most probably reject licensing their music for podcasts if it is not DRM-protected, since single songs could be extracted. And, commercial podcasts cannot use CC-licensed music, since the CC audio license is limited to non-commercial use.

We could imagine commercial, DRM-protected podcasts where DRM limits, for example, the number of plays and prevents the extraction of single songs. This would, on the one hand, make it easier for labels to license their music for podcasts, and on the other hand, not annoy consumers too much, since podcasts are not likely to be played many times and/or on different devices. It is rather the time-shifting feature and the automatic subscription that makes podcasts so attractive.

However, the prime problem of DRM technology today would strike here: lacking interoperability. One factor that makes podcasts so popular is the easy use of the MP3 format that is supported by a large variety of devices. Consumers will hardly accept DRM-protected podcasts that impair user experience – in particular if a parallel universe of free, unprotected podcasts exists.

Bottom line

Podcasting is one more step toward the disintermediation of media and is increasing diversity and customer choice. The format has already shifted from a pure amateur movement to being used as a marketing tool. It is still an open question, though, whether viable business models can be developed for paid podcasts. If podcasts are to incorporate music on a large scale, some use of DRM would be needed to make podcast licensing acceptable to music labels. As long as DRM systems are not interoperable and restrict user experience, however, DRM will be a no-go for podcast fans.

Sources

- BoKu Communications: http://www.bokucom.com
- Boyd, Clark (2005): Scot's podcast airs tartan talent. Online available at: http://news.bbc.co.uk/1/hi/technology/4606077.stm
- Broadcast Music Inc.: http://www.bmi.com
- Buckman, John (2005): Magnatune embraces podcasting. Online available at: http://www.podcastingnews.com/articles/Magnatune_Embraces_Podcas.html
- Creative Commons Audio: http://creativecommons.org/audio
- Didden, Carly (2005): A and B's of podcasting (too early for C's?) – Podcasting legal issues"; http://www.collegebroadcasters.org/podcast.shtml
- Forrester Research (2005): New report forecasts growth of satellite radio and podcasting. Online available at: http://www.forrester.com/ER/Press/Release/0,1769,996,00.html
- Knowledge@Wharton (2005): Podcasting: Can this new medium make money?. Online available at: http://knowledge.wharton.upenn.edu/index.cfm?fa=printArticle&ID=1239
- Podcasting News: http://www.podcastingnews.com
- Rubel, Steve (2004): Pondering podvertising possibilities. Online available at: http://www.imediaconnection.com/content/4735.asp

► Sixtus, Mario (2005): Verwirrung bei der GEMA. Online available at: http://www.sixtus.net/entry/389_0_1_0_C/

About the author: *Nicole Dufft* is a senior analyst at Berlecon Research. She has been analysing a variety of ICT topics ranging from mobile computing and application service providing to DRM. Currently, she works in the field "digital consumer". She is a member of the INDICARE project team.

Status: first posted 19/07/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=122

eBooks - The stony road to success and the role of DRM

By: Philipp Bohn, Berlecon Research, Berlin, Germany

Abstract: eBooks have already been dragged through their first hype cycle. Then, matters cooled off again. This was primarily due to highly expensive reading devices and a limited range of books on offer. This article takes a look at the technology infrastructure and digital rights in the e-publishing environment and introduces the reader to innovative business models based on DRM, but also concepts that work without protection.

Keywords: economic analysis – business models, consumer expectations, e-books, usage rights

Waiting for a miracle

eBooks may become really popular once affordable devices are introduced to the market and extensive libraries, including all the current bestsellers, are available for download. The introduction of the latest Harry Potter novel serves as a good example for the reservation of publishers and authors towards entering the eBook market (Rowling 2005).

The issue of eBooks has lately re-entered the spotlight of attention with the introduction of Sony's Librié. Since reader hardware made by Franklin, RCA, or Gemstar is no longer being distributed, the Librié is the first newly developed device to have entered the market for years. Its display closely resembles that of a real book. It can hold 10 MB of digital content, and costs ¥41,790 (about 320€ at Amazon Japan) (Lewis 2005).

DRM infrastructure

There is some confusion concerning the term *eBook*. We distinguish eBook content, eBook reader hardware and eBook reader software (cf. figure 1 next page).

If the reading hardware is *dedicated*, it is developed for the convenient consumption of eBooks. Regarding weight and readability, they try to emulate the experience of a real book.

Integrated reading hardware offers the technical capability to process eBooks. But in contrast to dedicated hardware, its use is not limited to reading. Personal Digital Assistants (PDAs), desktop computers, Tablet PCs and laptops can be used for reading eBooks. Mobile phones originally were not developed for reading, but technical advancement of screens, user interfaces, and memory continue to improve the potential of these devices for reading eBooks.

The capability of reading eBooks sometimes is even a *by-product* not intended by the manufacturer. This is for example the case with Nintendo's Game Boy or Apple's iPod. Featuring respectable screens, it is private developers who offer software to convert digital content into formats readable by these devices. The manufacturers do not support this, but do not hinder their development either.

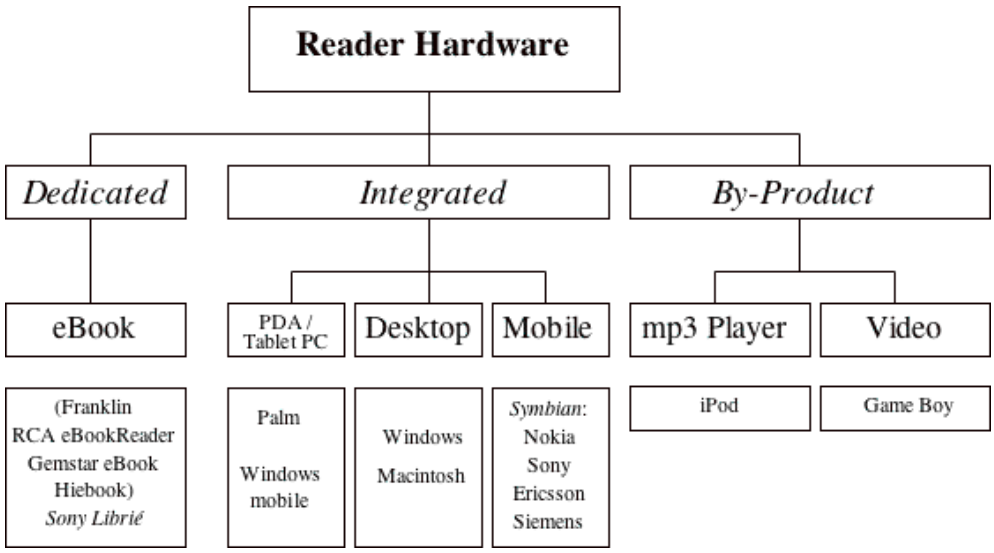


Figure 1: Digital devices capable of displaying eBooks

eBook reading software

Special software is required for reading eBooks. It comes pre-installed on a reading device or can be downloaded from the companies' websites. The basic version usually is free of charge. As each software format is linked to its own file format, there is no interoperability. For example, an eBook purchased in Mobipocket's file format cannot be read with Acrobat Reader (requiring pdf-files). Unfortunately, there is no single commercial reading device or software that can handle all the different file formats.

Acrobat Reader (Macintosh, Windows, Unix, Palm, Pocket PC, Symbian OS): Acrobat Reader's success rests heavily on the wide use of the pdf-format. The pdf-format is still without doubt the format of choice for desktop eBooks in many online bookstores. Nevertheless it is noteworthy that Adobe's Content Server DRM system has been discontinued as of November 2004. It has been replaced by the LiveCycle Policy Server solution. This move indicates that Adobe is abandoning DRM-solutions for publishers, concentrating on the enterprise documents market (Rosenblatt 2005).

eReader (Macintosh, Windows, Windows mobile, Palm): The eBook store of the same name has developed this software primarily to support their own file format. It also works with Palm's document format. In order to activate a commercial eBook, a special code is required. It is generated using the credit card number the customer has given to purchase the book.

Microsoft Reader (Windows, Tablet / Pocket PC): In order to read DRM-protected eBooks, the reading software needs to be activated via Microsoft's website. Using a single account, the consumer can activate up to six devices. There can be activation problems if the customer uses a new device and wants to read books purchased with older versions of the software (Rothman 2003). Quoting a major publishing company's representative, they do not support this software, because "it is not even supported by Microsoft themselves".

Mobipocket (availability: Macintosh, Windows, PalmOS, Psion, Symbian OS): The French company Mobipocket has developed the software primarily for PDAs. Upgrading the free basic software allows the user to define usage rights for non-commercial use. Commercial publishers use Mobipocket's eBookbase to protect and distribute digital content. A wide range of international retailers and platforms supports this software.

Of the major eBook distributors in Germany (Amazon, bol, ciando, libri, pdassi), three support Acrobat Reader, one supports eReader and Mobipocket respectively. In the desktop environment, Acrobat Reader is the

common standard, while the decision is still open in the portable environment.

Usage rights and their influence on eBooks' success

Primarily, usage rights that are controlled by the DRM system comprise: Print content, add notes, copy / paste, period of usage, extract or add single pages and authentication of reading hardware and software. Problems arise mostly with the period of usage and authentication. The authentication scheme sometimes requires a code composed partly of the customers´ credit card number. Consumers may feel rather reluctant to accept this policy.

Sony's Librié, which is without doubt technologically very sophisticated, is an example of how great platforms and the advantages of digital content can become almost useless for the consumer through DRM. Apart from featuring a price not suitable for mass marketing, only eBooks protected by Sony's proprietary Open MG DRM technology are available at the dedicated download store. There is a selection of a mere 200 volumes to date.

The files are set to expire after two months upon authentication. So the consumer is forced to read the book within that period of time. Given Librié's price tag, it seems unlikely that consumers will accept this (Lytle 2004). The company has reacted to the format problems, allowing for conversion of pdf-files into the Sony's proprietary BBeB-format (cf. Dynamism.com)

Applying DRM to the consumer's benefit

Once the technical issues described are resolved, existing online retail business models can be enhanced using DRM. And there are business models that can only work with the help of DRM. Also, substantial differences exist based on whether a book is used for entertainment (e.g. novels), education (textbooks, encyclopedias) or orientation (travel guides).

Term-lease: While limited usage rights (e.g. expiry after two months) are hardly tolerable with novels, they can make sense in the educational environment. In case a student needs to buy a book for a course at university, its expiry after a predefined period of time might not be a problem. After all, upon successfully passing an exam, the textbook is hardly needed much longer, or becomes outdated. Thus, stricter usage rights along with a reduction in price can be in the mutual interest of both parties.

Course-packs: If the consumer opts for longer use, updates can be delivered digitally upon publication. Also, the customer can buy content chapter-wise, which would be impossible with traditional books. Publishers could sell "course packs" existing of individual chapters, articles and multimedia content (Vaknin 2005).

In Asian countries such as Japan or South Korea, there are providers offering eBooks on a subscription basis: Japanese publisher *Shinchosha* delivers serialized novels daily throughout the workweek to consumers´ mobile phones in chunks of 1,000 to 1,200 characters at a price of about ¥100 (0,75 €) per month. After a short time, they cannot be accessed any more. Yet, due to technically sophisticated screens and longer commutes, this services is starting to become widely accepted (Fitzpatrick 2004).

DRM and the interplay with the operating system

Digital media can also be of great benefit for referential and encyclopedic use. In Germany, the popular *Duden* and *Brockhaus* – the leading multi-volume dictionary and encyclopedia – are available for desktop computers and PDAs.

On the upside, consumers carry with them large amounts of knowledge and easily access them even on mobile devices. Also, there is a steep reduction in price, because of the much lower production cost for reference works of such large volume. It is also easier to access single entries. Volumes can be updated on a regular basis.

But there can be problems concerning the interplay of the DRM and operating systems involved. To give an example concerning the Brockhaus Encyclopedia: If customers update Windows XP using service pack 2, the DRM system is blocked and the program

cannot be executed any more, due to downward compatibility problems. In order to fix this problem, Brockhaus offers a lengthy "how-to" guide. A patch must be downloaded and installed on the computer. While this is still a nuisance to the tech-savvy user, it can be prohibitively disadvantageous for the average customer.

Existing DRM systems are not suitable for every product

Gate5 offers navigational applications that can be integrated with guides to major German cities. Partners with experience in the publishing of travel literature provide the content. Supported devices are Symbian Series 60 and 80 mobile phones, MS Windows Mobile Smartphones, Pocket PC and the Palm PDA. The company has developed a proprietary DRM system, as existing solutions are not capable of securely delivering products that are bundles of diverging formats like text, video and pictures.

Doing without DRM

Independent publishers such as *Baen Books* rely on mutual trust and the quality of their content rather than active DRM. Baen's books are released without any DRM protection and are often made accessible as free downloads for promotional purposes. Readers buy an actual book in case they liked the free digital version. For independent publishers, wide exposure of their content is a prime promotional tool.

There are also individual works published under a Creative Commons license. Examples are the science-fiction novels by Canadian author *Cory Doctorov*. While everyone is free to download them from his personal website, they are also on sale at major digital retail outlets and actual bookstores (Cf. Sources). The underlying idea is that the best promotion for a book is itself.

Conclusion

DRM holds opportunities and threats for the popularity of eBooks. There are technical issues to be resolved, e.g. concerning software and operating system updates and downward compatibility. Necessary updates should be more concerted with content providers and developers of DRM technologies.

DRM can hold benefits for both publishers and consumers. There is great promise if it is able to provide flexibility for the various forms of eBooks. Expiry could be set according to customers' needs, resulting in greater demand for more flexible products coming with a lower price. Due to similar experiences in the "real" world (e.g. lending books, subscribing to magazines), consumers are more likely to accept DRM limiting usage rights. Content that could hardly be distributed before – such as serialized novels – may become real business due to digital distribution.

Bottom line

Until basic problems – interoperability, support of different eBook formats and their DRM systems, affordability and choice of eBook reading hardware – are resolved, the breakthrough of eBooks will be further delayed. But there are some business models that would make DRM acceptable for consumers.

Sources

- Mr. Doctorov's novels are available for download at http://www.craphound.com/novels.php
- Dynamism.com: http://www.dynamism.com/libríe/
- Fitzpatrick, Michael (2004): The big read. In: New Media Age, May 13, p. 23
- Gate5: http://www.gate5.de/index_en.html
- Lewis, Peter (2005): Prose and Cons: Sony´s new e-book. In: Fortune (Europe), Vol. 150, I. 4, p. 28
- Lytle, J. Mark (2004): Library without books. In: Guardian Unlimited. Online available at: http://books.guardian.co.uk/print/0,3858,4906744-110368,00.html
- Rosenblatt, Bill (2005): Publishers: Want DRM? Then pay for it. In: Seybold Report, Vol. 4, I. 22, p. 18
- Rothman, David (2003): NetWorker on the follies of today's DRM. Online available at: http://www.teleread.org/blog/?p=2546
- Rowling, Joanne K. (2005): Harry Potter e-Book scam. Online available at: http://www.jkrowling.com/textonly/news_view.cfm?id=84

► Vaknin, Sam (2005): Digital object identifiers and the future of online content – Part II. 07.12.2005. Online available at: http://www.webpronews.com/ebusiness/contentandcopywriting/wpn-6-20050712DigitalObjectIdentifiersandtheFutureofOnlineContentPartII.html

About the author: After having graduated from University of Mannheim (Business Administration), *Philipp Bohn* has joined Berlecon Research as Junior Analyst. He is a member of the INIDICARE team. Contact: pb@berlecon.de

Status: first posted 29/07/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=127

TIRAMISU: That's unobtrusive DRM in the home domain

By: Boštjan Marušič, University of Ljubljana, Ljubljana, Slovenia; Philippe de Cuetos, ENST, Paris, France; Laurent Piron, Nagravision, Lausanne, Switzerland; Zvi Lifshitz, Optibase, Herzlia, Israel.

Abstract: Media delivery over heterogeneous networks requires both flexible representation and robust protection of content. This article provides details on the framework for audiovisual content creation, delivery, consumption and protection as conceived within the European Union's IST project TIRAMISU (The Innovative Rights and Access Management Interplatform SoIUtion). The proposed framework supports multi-media, multi-channel distribution, consumption on multiple devices in home domains, and allows for super-distribution. The Digital Rights Management (DRM) scheme claims to be unobtrusive.

Keywords: project description – authorized domain, interoperability, smartcard, superdistribution, privacy, technical protection measures – EU

The context of the TIRAMISU framework

Convergence of digital media distribution channels and content representation formats has the potential to provide significant benefits to content owners and users alike by changing traditional content distribution and consumption patterns. Content that has initially been delivered over digital broadcasts can be further distributed over the Internet or through pervasive peer-to-peer (P2P) networks and consumed on a variety of consumption devices. Content providers are rapidly gaining awareness of the importance of multi-channel delivery of content, by which a potentially larger customer base can be targeted (Lauchlan 2001). At the current stage, content providers address each delivery channel independently of others by preparing content in a way that is specific for that channel. Protection methods that enforce consumption policies are also targeting specific requirements of a distribution channel. Opposed to this approach, multi-channel delivery allows preparing content for some display characteristics and content can be obtained either on, for example an IP network or a removable device. At consumption, if necessary, adaptation of content can be done. While multi-channel delivery has the potential to increase the owner's revenue streams, content owners are becoming increasingly concerned in view of the innumerable possibilities for illegal consumption and distribution, P2P networks being the most highlighted threat.

Integration of DRM technology with alternative distribution channels such as P2P networks may provide the solution for crossing the fine line between embracing functionalities that users want and at the same time maintaining control over Intellectual Property Rights (IPR). A simplified DRM system (Figure 1) relies on media scrambling for protection. The privilege to consume protected content is granted to the end-user by a license, which specifies usage terms and conditions and includes the key(s) needed for content descrambling. The process of transferring scrambling keys between the content scrambling node and the rendering node is denoted by the term *key management*.

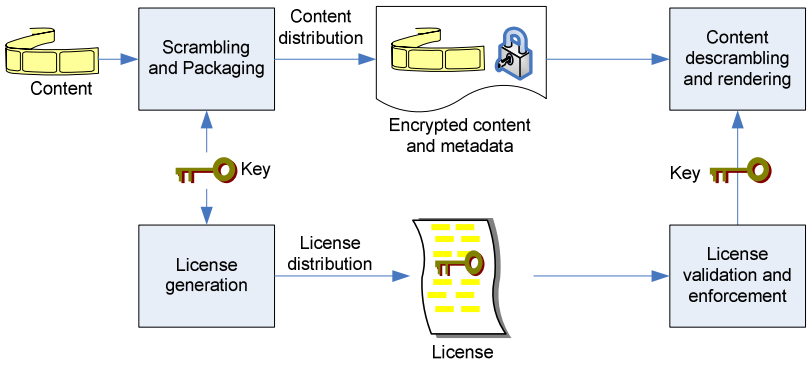


Figure 1: Architecture of a generic DRM system

Integration of media distribution and DRM is key to implementing content super-distribution. Super-distribution is an online retailing scheme that encourages free and widespread distribution of digital objects that can only be consumed under a restricted set of circumstances. Super-distribution is a distribution scheme where consumers are involved in the process of C2C (consumer to consumer) distribution of content initially acquired through B2C (business to consumer) distribution channels. For IPR protection reasons, content must be super-distributed in scrambled form. This implies the need for a DRM system that provides the means to acquire consumption rights and descrambling keys on one hand and enforcement of those rights on the other.

MPEG-21, which is the last in the series (MPEG-1,-2,-4,-7) of MPEG standards (cf. Burnett et al. 2003; Bormans and Hill 2002; Bormans et al. 2003) defines a normative open framework for interoperable multimedia delivery and consumption that is based on two essential concepts: the definition of a fundamental unit of distribution and transaction (the Digital Item - DI), and the concept of users interacting with DIs. A DI is a structured digital object with resources, unique identification and metadata, where the structure of the DI implies relationships among parts of the DI, i.e. the resources and metadata.

The TIRAMISU approach

The framework proposed by TIRAMISU is based on the MPEG-21 standard for multimedia content delivery and consumption and at the same time it complements it in several aspects, most notably by fully specifying a Digital Rights Management (DRM) scheme. Central to the described framework is a novel Key Management System (KMS), relying on smartcards, which addresses many issues that previously blocked wider adoption of DRM: obtrusiveness of the DRM technology perceived by the end user, flexibility in license formulation and adequate level of trust as requested by content owners. The TIRAMISU framework intrinsically supports the concept of super-distribution.

The central objective of the TIRAMISU project is to create an environment, in which content providers can deliver content to users over multiple distribution mechanisms to a variety of consumption devices, with confidence that imposed usage policies will be respected. At the same time TIRAMISU balances between insuring proper compensation to Intellectual Property (IP) owners and reasonable user expectations. *TIRAMISU approaches this by motivating content distribution policies that do not imply restrictions on further content proliferation (P2P networks, for example), but stipulate compensation for content consumption only*. TIRAMISU is consequently a super-distribution framework. Such philosophy is based on the conviction that doing so within the context of interoperable DRM systems, content will reach a larger number of potential customers to the benefit of providers and consumers. In this respect the TIRAMISU approach clearly contrasts the philosophy of established content protection policies that rely on copy-

protection and forward-lock mechanisms to prevent C2C distribution.

A major requirement to be addressed when dealing with multi-channel delivery is interoperability both in terms of content representation and DRM. Within TIRAMISU this is addressed by relying on open standards (MPEG-4, MPEG-21 and ISMA – International Streaming Media Alliance). Content is abstracted as a Digital Item (DI) and in this form traverses diverse delivery channels and is consumable on a variety of devices. Since convergence to a single set of standards is unlikely, TIRAMISU also explores how bridging between delivery channels and DRM systems can be achieved.

Home domain, networked devices

Central to the TIRAMISU framework is the concept of home domains, in which content may circulate between different devices, e.g. from the living room hi-fi system to the car stereo, to the MP3 player. Content usage policy enforcement at the end-user side is left to hardware in form of smartcards. Smartcards also provide the link between the user and the home domain concept. The TIRAMISU user may own several smartcards that are registered to a particular home domain and can be used on any compliant device.

Conceptually the set of devices belonging to a user or a group, for example a family, forms a personal space where content may circulate. This concept implies that content rights purchased for a piece of content are persistent over all devices of the home domain. Eventually, from the content consumption perspective there is no difference whether the user owns one or several devices (Figure 2).

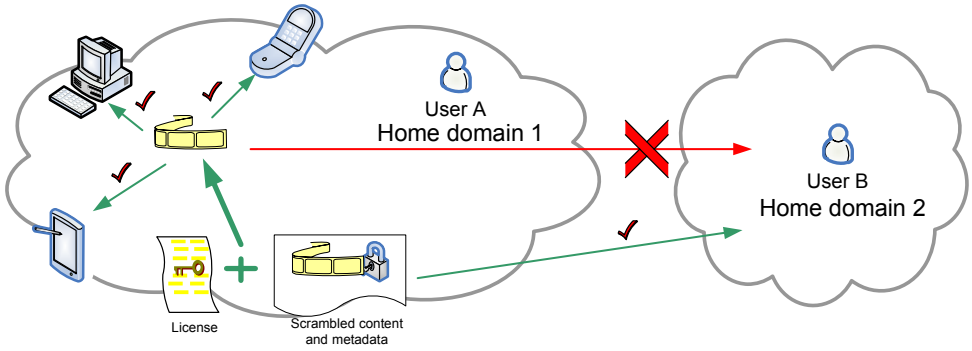


Figure 2: The concept of home domain

Technically the concept of home domain opens several issues due to the fact that rights pertaining to a DI are not bound to a single device or to a single smartcard. Consequently a mechanism for guaranteeing that the same set of rights is persistent on all devices of the home domain is necessary. Additionally, content must be adapted to fit the diverse rendering capabilities of each consumption device.

While smartcards can guarantee that a descrambling key is provided only when a right exists, the device that is using this key is also an important part of the system. Some rules are necessary in order to make this device compliant with TIRAMISU. Depending on its capabilities, these rules can be more or less restrictive. The extreme case is for a device allowing to trans-code content, as in this case it manipulates clear content. The framework could be extended to include some revocation rules for devices.

TIRAMISU architecture extends beyond other initiatives and their definition of the home domain concept by providing wider support for redistribution of content through super-distribution independent of the distribution channel, where the actual C2C distribution is conceptually distribution of content from one home domain to another.

TIRAMISU framework architecture

Figure 3 provides a block diagram of the TIRAMISU framework architecture with the basic content flows through the system. The TIRAMISU architecture is based on the prin-

ciples that content in the framework is represented as an MPEG-21 DI. The architecture in Figure 3 identifies the five main entities in the system each with a specific role: the content author, the content owner, the content distributor, the license distributor and the end-user or content consumer. The content author is the entity that authors the media resources and transfers its IPR over to the content owner. The content owner is responsible for specifying the consumption terms and conditions and selects target distribution mechanisms over which the DI will be distributed. With a particular license termed sharing license, the content owner delegates the process of license distribution to a selected license distributor, which is responsible for issuing domain licenses to end-users. Eventually, the content distributor delivers DI comprising the resource suitable for a target usage environment to the end-user.

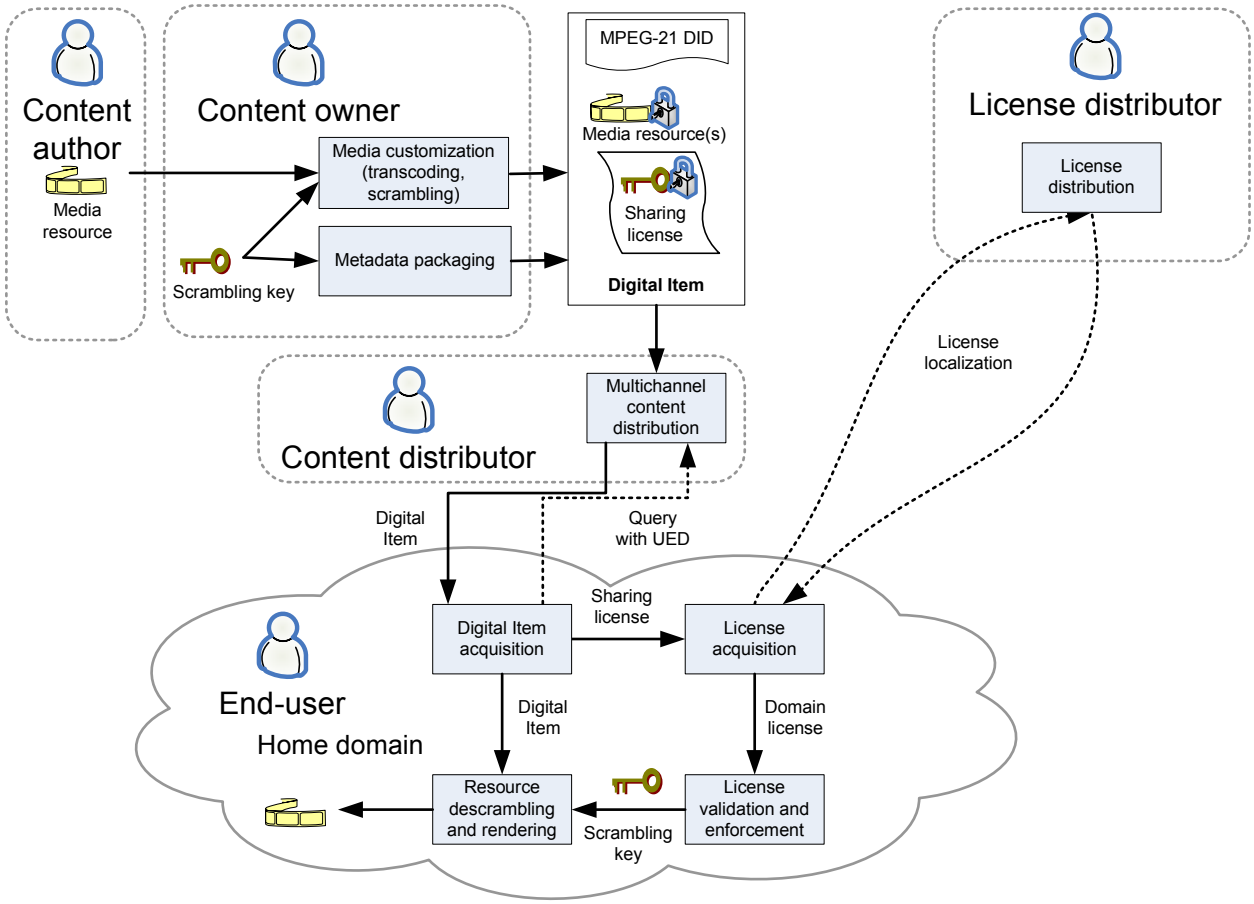


Figure 3: TIRAMISU architecture

TIRAMISU features and properties

Smartcards and home domain management

A home domain is a group of devices that feature the same set of rights in terms of content consumption. In TIRAMISU the process of license enforcement is delegated to smartcards. All smartcards belonging to a particular home domain share a cryptographic secret that is essential to enforce consumption licenses. Before a smartcard becomes usable in the context of a home domain it must be registered with the home domain manager. All smartcards registered to the same domain and consequently sharing the same cryptographic secret are able to enforce licenses issued to their domain. In other words if a license was bought using one smartcard, the associated DI can be consumed on all other devices with a smartcard belonging to the same home domain.

Super-distribution between home domains

Once the end-user has obtained the domain license, he has the right to consume the associated DI on all devices belonging to his home domain as the smartcards of the home domain can access the descrambling key

from the domain license. Additionally, the DI can freely be super-distributed to other home domains, as the descrambling key embedded in the domain license that is issued for a particular home domain can not be read by a smartcard which does not belong to that domain.

The importance of smartcards
Smartcards represent a secure element in an insecure environment. Smartcards in home domains provide a secure repository for home domain secrets and are the elements that enforce the domain license by validating it before providing the content descrambling key to the rendering device. Compared to software-based solutions, the smartcard being a hardware device is more difficult to compromise and it thus offers an increased level of security.

User anonymity
The TIRAMISU KMS may under certain circumstances guarantee complete end-user anonymity and privacy. Domain licenses are issued to home domains not end-users. The end-user only needs to expose his identity to enable billing related to license acquisition. However, in cases when smartcards also serve as a mechanism for payment (pre-paid smartcards), the end-user anonymity and privacy can be guaranteed.

Is TIRAMISU the next hot technology?

DRM frameworks, such as Windows Media and iTunes, already exist, with a certain degree of success. They have not swept the media world because they are based on proprietary technology that targets closed systems. The success of the TIRAMISU concept depends on its acceptance as a worldwide open international standard. There are several key factors that might accelerate or block such acceptance, namely:

Acceptance by content providers. This is probably the biggest hurdle. The movie industry does not have a good record of adapting to new technology. Back in the 1980s, the movie industry faced a new technology that supposedly threatened its bottom line – the VCR. The threat looked so alarming, that *Jack Valenti,* the long time head of the Motion Picture Association of America (MPAA), compared the VCR to no less than the Boston Strangler, and the MPAA took the battle against Betamax to the US Supreme Court.

Fortunately for everybody involved, the MPAA lost the battle. The Supreme Court accepted the right of fair-use coping, and ruled against the movie industry. We all know what happened to the VCR: not long after that defeat, the studios discovered that tape rentals were even more of a cash cow than movie tickets. We are probably in the same situation now. The movie industry is already resorting to legal actions against the new technology. Hopefully legal systems will learn the lesson quicker than the industry and will refuse to cooperate with its strategy, leaving it no choice but to embrace technology instead of fighting it.

Acceptance by consumers. Assuming the pervasiveness and ease of illegal file sharing, it initially seems difficult to expect that the consumers, being used to cost-free media consumption, will be motivated to revert to a paying system. However a deeper analysis of the situation reveals that cost is not a major factor. If the cost is right, and the protection measures are unobtrusive, an atmosphere of legal business will be created and most consumers will be happy to be part of it. Just like people are happy to tip for a service or voluntarily deposit the cost of the evening newspaper in the open box.

Acceptance by media distribution industry. The move from B2C to C2C means less business for the Businesses, which are expected to battle such a move. Eventually they will need to accept market reality and adapt their business accordingly. The businesses which display the flexibility to adopt new technologies for inventing new business models based on service aggregation will prevail, just like the emergence of tape rental shops didn't obliterate the movie theatres.

Emergence of a single standard. This is a key factor in accelerating the acceptance of the three market segments referred to above. TIRAMISU tries to show the way by picking from existing standards, but the same concept can be realised with a different set or variations of standards. This will not be regarded as a failure since the importance of

the framework is in its concept rather than the implementation details.

Worldwide embrace of smartcard technology. This actually has already happened. Smartcards are already embedded in cellular phones, which are rapidly evolving into integrated media players. Many PCs already shipped equipped with smartcard readers. The ease and cost of incorporating smartcards in every media consumer device is minimal.

Tamperproof technology. One may claim that in order for a DRM system to succeed it has to prove to be tamperproof, and since such a proof has to persist over time, the adoption of the technology must be delayed. However the state of the market demonstrates that immunity of systems to bypassing is not a major issue. Consumption is not a zero-sum game. As with the VCR, legal and profitable business continues to thrive despite fraudulence. In many cases the fraudulence helps the promotion of the profitable business. There is little doubt that unobtrusive DRM can sweep the market.

Bottom line

The end-to-end framework for content creation, delivery and protection as conceived within the IST-TIRAMISU project is independent of the distribution channel. It is based on open standards such as MPEG-21 and ISMA and provides full support for super-distribution. The increased security of the framework is a consequence of the application of smartcards for the manipulation of sensitive data. From the consumer's point of view, the TIRAMISU framework provides several features rendering the DRM system unobtrusive.

Sources

- Lauchlan, S. (2001): Content is king. *Internet World*, November 2001
- Burnett, I, van de Walle, R.; Hill, K.; Bormans, J.; Pereira, F. (2003): MPEG-21: Goals and achievements. *IEEE Multimedia*, vol. 10, no. 4, pp. 60-70, October/December 2003
- Bormans, J. and Hill, K.: MPEG-21 overview v.5. ISO/IEC JTC1/SC29/WG11, Shanghai, October 2002
- Bormans, J.; Gelissen, J.; Perkins, A.: MPEG-21: The 21st century multimedia framework. *IEEE Signal Processing Magazine*, pp. 53-62, March 2003
- TIRAMISU web site http:// www.tiramisu-project.org
- Marušič, Boštjan; Dobravec, Štefan; de Cuetos, Philippe; Concolato Cyril; Piron, Laurent, Tasič, Jurij F.: TIRAMISU: A novel approach to content representation and key management for seamless super-distribution of protected media; to be published in "Signal Processing: Image Communication, Special Issue on European projects on visual representation systems and services", Fall 2005.

About the authors

Dr. Boštjan Marušič is a full-time researcher at the Laboratory for digital signal processing of the University of Ljubljana. His research interests include wavelet image and video coding, telecommunication systems and networks, Internet. Contact: bostjan.marusic@fe.uni-lj.si

Philippe de Cuetos is a research scientist who is designing and implementing innovative services for multimedia content management. He holds a PhD from ENST and has recently joined Expway. Contact: philippe.de-cuetos@expway.com

Laurent Piron works at Nagravision. His main focus is on mobile television. He has 10 years experience in video compression and conditional access on TV systems. Contact: Laurent.Piron@nagra.com

Zvi Lifshitz is a senior software architect in Optibase. He is a major contributor and the representor of Israel at the ISO's MPEG committee, where he has led the IM1 Software Platform group and now participant in MPEG-21 and MPEG-A workgroups. Contact: zvil@zvil.com

Status: first posted 27/07/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=125

ODRL Workshop 2005 Report

By Susanne Guth, O2, Munich, Germany, Renato Iannella, NICTA, Brisbane, Australia, and Carlos Serrão, ISCTE and Adetti, Portugal

Abstract: This article is a report by the chairpersons of the second international ODRL Workshop 2005, held in Lisbon, Portugal on 7.-8. July 2005. It highlights topics which presumably will interest INDICARE Monitor readers most. Nevertheless, all keynote talks, invited talks, paper sessions, and the open panel are covered. The last paragraph gives a résumé of the last year's activity and future work of the ODRL initiative.

Keywords: conference report – Creative Commons, identity management, interoperability, mobile DRM, patents, rights expression language, trusted computing

Introduction

Rights expression languages provide a metadata framework for the expression of rights for any kind of digital media content. ODRL, the Open Digital Rights Language, an XML-based rights expression language (REL) is hosted by the *ODRL Initiative*. The Initiative has gained international significance in the field of digital rights management (DRM) over the past years, culminating in ODRL being adopted as an international standard by the Open Mobile Alliance for supporting the process of mobile content distribution and management.

In order to bring together the research and industry communities to share experiences and discuss the future developments of the ODRL language the ODRL Initiative organises workshops. The first International ODRL Workshop was held in Vienna, Austria in April 2004. This year's international ODRL Workshop 2005 took place in Lisbon, Portugal from 7th to 8th of July 2005. The present report highlights topics which presumably will interest INDICARE Monitor readers most. A comprehensive report about the workshop is available at the ODRL website (http://odrl.net/workshop2005/).

Keynote talks

Identity and content rights
Simon Nicholson, Director, Wireless Business Strategy & Development, Sun Microsystems

When *Simon Nicholson*, supporter of the Liberty Alliance (a consortium of 150 members throughout the IT and communications industry) looks years ahead he does not see himself carrying around several devices, such as a phone, a PDA, or a blackberry; nor will he possess several keys, several credit cards, or other identity cards. He will have one tiny device that authenticates him as he moves "through space". It will open his front door, receive all incoming calls and e-mails, grant access to his company's premises and withdraw money from his bank account. Simon Nicholson brings it to the point: In the future, all that matters in identification. Services will be bound to an identity rather than to a specific device, such as an iPod or a mobile phone.

According to Nicholson, the combination of *value*, *trust*, and *privacy* will determine future digital services. Trust is the key driver of the online model and identity management is the key enabler for trust. Identity management requires interoperability but also helps to remove single points of failure. To enable identity management the Liberty Alliance has developed a technical architecture and the Identity Service Interface Specification. Specifications need implementation and testing and that's what is currently on the way with e.g. OMA members.

Where does that all connect to ODRL? First of all, ODRL needs to support the integration of the Liberty identification schemes in the language with regard to meta data and data models. Second, ODRL needs the expressiveness for different levels of privacy to be

"Liberty compliant". For example, content that defines me, such as credit card details and health records need a higher level of protection than maybe contact details on my phone. The two initiatives will keep on working closely together on this topic.

OMA DRM 2.0 status and future work
Jan von der Meer, OMA DRM WG Leader & Philips Electronics

The route from OMA 1.0 to OMA 2.0 was presented in The INDICARE Monitor in August last year (Buhse 2004). The present status was reported at the ODRL Workshop. The Open Mobile Alliance (OMA) currently has about 200 members. Version 1.0 of the OMA standard is targeted at light media and offers lightweight DRM. Currently, over 250 handsets models are on the market with OMA DRM Version 1.0 support. The rights objects that are used for the separate delivery mechanism are expressed in ODRL.

OMA DRM Version 2.0 is a much more comprehensive and complex DRM for premium media. It supports additional concepts, like domains and additional security concepts, such as a public key infrastructure regulated by the independent Content Management License Administrator (CM-LA). The next DRM (interoperability) test fest is to be held in September in Seoul to move the specification forward to "enabler release" status. However, the DRM WG Leader, Jan van der Meer did not reveal any detailed schedule for when OMA DRM Version 2.0 will be approved or if further test fests are planned.

OMA DRM Version 2.0 is not restricted to mobile communications but supports the convergence between the mobile world and PCs. This might explain the positive market forecasts by CoreMedia foreseeing that in 2007, 60 % of the globally protected content will use OMA DRM and that mobile content revenues will have increased to almost US $ 30 billion pa. On the OMA roadmap are DRM extensions for e.g. broadcast (TV), support of removable media (technology that goes beyond domains), and more OMA (desktop) clients for various platforms.

DRM coordination work on IST FP6 NAVSHP projects
Miguel Dias, Adetti President, Portugal

The European Union, aiming at taking European Research and Development a step forward, organises co-ordination meetings among the different 6th-Framework-Program (FP6) R&D areas and projects. In the area of Networked Audio Visual Systems and Home Platforms (NAVSHP), four different co-ordination groups have been established:

- CG1 - Digital Rights Management,
- CG2 - Quality of Service in a Convergent Environment,
- CG3 - In-Home Networks and Platforms and
- CG4 - Content Media Processing.

Delegates from six FP6 Projects (Medianet, Enthrone, Tiramisu, Danae, Avista, and Visnet) enlarged by the FP5 Project ELIN (chaired by *Miguel Dias*) and participation from the European Broadcasting Union have joined efforts in the framework of Coordination Group 1 – CG1 – DRM (chaired by *Leonardo Chiariglione*). They work on a *DRM Requirements Report* that expresses the common view of NAVSHP on DRM and the requirements for future DRM technologies, systems and toolkits in the European audiovisual sector. The authors are planning to submit this report for consideration of other FP6 Priorities, so that it may achieve the status of a DRM Requirements Report for the complete FP6 programme.

Miguel Dias, chairman of the CG1 – DRM presented the coordination group and the current status of the Requirements document which has currently around 100 requirements (subdivided in business and market requirements, technological requirements and socio-economic requirements). He also announced that the group is currently receiving comments from several external sources (Intel, IFPI, MPAA, etc.) and has encouraged the ODRL Initiative to also contribute to the document.

Paper Sessions

Formalising ODRL Semantics using Web Ontologies
Roberto García, Rosa Gil, Isabel Gallego and Jaime Delgado

A new approach to interoperability between ODRL and MPEG-21 REL
Jaime Delgado, Jose Prados, Eva Rodríguez, University Pompeu Fabra

---

Translation from one rights expression language to another is an important topic. Anecdotal evidence is that CoreMedia has built an OMA plugin (ODRL based) for the Windows Media Player (MPEG REL based) (cf. CoreMedia 2005). The University Pompeu Fabra in Barcelona presented two contributions in this field.

In the first paper the need for a rights expression language ontology was discussed. With such ontologies, representing the generic namespace of rights expression languages, a common base could be created where different languages can be mapped onto and thus translated from one to another. The second contribution showed how a translation can be done from OMA DRM 1.0 and 2.0 ODRL profiles to MPEG REL with the help of XSLT processing.

A Review of the OMA DRM V2 ODRL Profile
Renato Iannella, NICTA, Australia

This paper presented a review of the OMA DRM Version 2.0 profile of the ODRL REL. It looked at the decisions made by the OMA DRM working group and offered alternative solutions. Some of the issues highlighted included the use of the inheritance model (for subscriptions) and the impact on recording the current state of time/count based constraints, and the effect of super-distribution on privacy without the explicit "tracked" requirement in the ODRL agreement. *Renato Iannella* concluded that the lessons learned are important for both the ODRL Initiative and for other groups developing profiles of the ODRL REL. In particular, he noted that OMA and the ODRL Initiative need to formalise their relationship to enable sharing of issues that are directly related to the ODRL profile.

Extending ODRL to Enable Bi-Directional Communication
Alapan Arnab, Andrew Hutchinson, University of Cape Town

The paper discussed an important issue in the field of rights expression languages: how to negotiate rights. The current versions of rights expression languages ODRL, XrML and MPEG REL stress the granting of rights from the rights holder to the user. This might be a reason why current rights expression language initiatives do not include the negotiation of rights.

Alapan Arnab showed a theoretical approach to how the negotiation aspect can be incorporated as part of a rights expression language. He stated that his proposed changes enable the end user to request changes to an offer or proactively request rights for a digital product. However, there has to be a clear distinction between the rights expression itself and the protocol for exchanging and negotiating rights expressions. Do the negotiation elements have to be part of the expression language? Clearly separating the requirements for a negotiation protocol and a REL that enables negotiation would be a valuable topic for future work in this field.

Using ODRL to express rights for different content usage scenarios
Carlos Serrao, Miguel Dias and Jaime Delgado, Adetti/ISCTE, Portugal and University Pompeu Fabra, Spain

---

Carlos Serrão provided a paper in which several ODRL usage examples are presented, stressing the fact that ODRL represents an opportunity to have rights expression richness, flexibility and at the same time openness. He addressed those characteristics in the ODRL language by providing examples of how ODRL is currently being used in several content usage scenarios, such as music download and streaming, video-surveillance data streaming and storage and remote sensing of JPEG2000 images.

This paper also makes a short reference to the OpenSDRM architecture, an open DRM

system that uses ODRL as its rights expression language and providing an interoperable rights enforcing layer. This layer acts as middleware to enforce the expressed rights over the content, through the provision of the Digital Wallet concept. The module which implements this concept is capable of accessing the rights locally or over the network, interpreting and enforcing them for the requesting content applications.

Embedding ODRL Statements in Dublin Core
Enric Peig and Jaime Delgado, University Pompeu Fabra, Spain

Enric Peig motivated the need for a human readable translation of rights expressions. He investigated the concrete usage of rights expressions within the Dublin Core metadata. He presented what a translation of rights expressions would look like and suggested a proper location for the translation within the Dublin Core metadata. For future work he envisaged a concrete approach to the automatic translation of ODRL rights expressions into a proper (English) sentence without losing important semantics.

Predicting the evolution of digital rights, digital objects and DRM languages
Jonathan Schull, Rochester Institute of Technology, USA

Jonathan Schull shared his long-standing knowledge about the evolution of digital goods, i.e. the virtualisation of the world and his visions for the future. He makes the very striking connection between the virtualisation of money and now, a few years later, the virtualisation of digital goods or information products.

From his experience of the early days of superdistribution and the observation how digital rights management technology has evolved, today he encourages distribution of content and copying of content rather than locking it in with strong security means, such as some of the current DRM technology. This approach keeps customers away from digital goods, Schull stated. He suggests to track superdistribution activities and to reward users who actively redistribute content, a concept that the OMA Version 2.0 specification already offers. He also sees the need to formulate rights that are valid downstream, i.e. rights that apply to the customer's customer. The ODRL Version 2.0 model allows for such downstream rights with the "Next Rights" concept and thus, it seems the technical means are available for a slightly different approach to DRM.

Invited talk

Plans, scope, and objectives of the GeoDRM WG within the Open Geospatial Consortium
Roland Wagner,University of Münster, Germany

The Open Geospatial Consortium (OGC) is a non-profit organisation with 250 members from the US, Europe, and Asia leading the development of standards for geospatial and location based services. The need for rights management in the geospatial sector results from the variety of information that is available for one location, e.g. information on infrastructure, industrial buildings, landscape, natural cover, etc. For future sophisticated location based services this information has to be brought together and at this point DRM is needed. The providers of the different types of geospatial information need a mechanism to protect and preserve their rights when their information is integrated.

The GeoDRM working group is part of the OGC. Its aim is to reuse digital rights technologies and to extend them to geospatial data handling and services. In the long run the group is aiming at integrating geospatial information automatically by interpreting DRM licenses reflecting the conditions of each geospatial information provider. In the development process of its specifications the GeoDRM working group will investigate ODRL as a REL candidate for the GeoDRM Reference Model and to formulate licenses for geospatial data.

Open panel

The impact of DRM Patents on REL Research and Standards
Susanne Guth, O2 Germany, Renato Iannella, NICTA, Australia

The authors of this article presented the view of the ODRL Initiative on the licence claims by MPEG LA with regard to rights expression languages. An article on this topic has been published in the INDICARE Monitor (Guth and Iannella 2005). It comprises a detailed analysis of the MPEG LA claims and highlights alternative views on the technical claims and prior art in the case of rights expression languages.

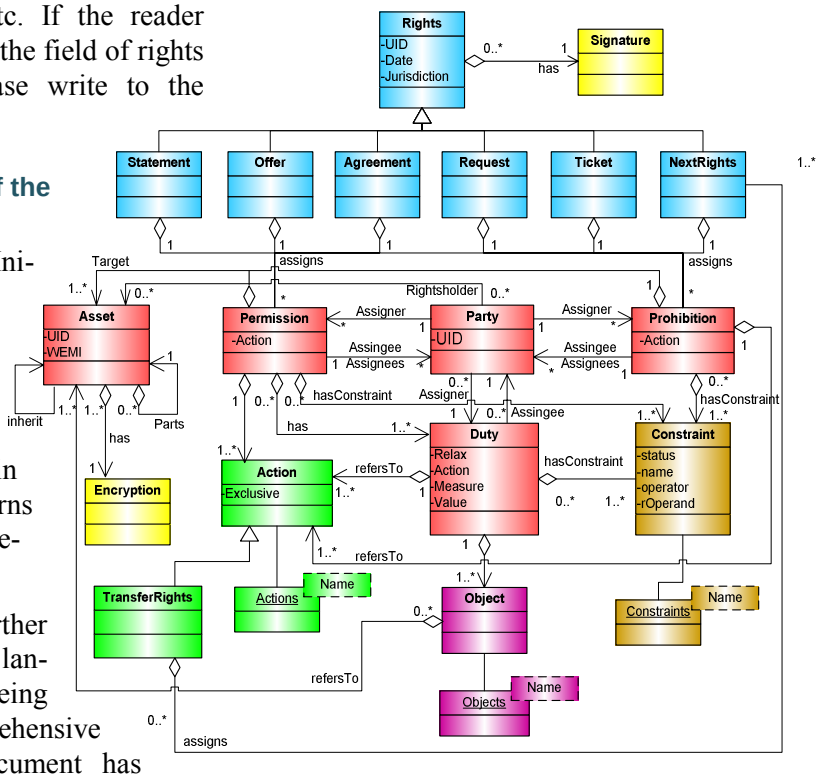
The negotiations between MPEG LA and e.g. the GSMA have not been settled yet. The GSM Association still regards the requested fees of 65c US $ per device and 25c US $ per user per year as not acceptable and not applicable for the mobile communications market. The only way to address the MPEG LA claim would be for each single patent to be technically investigated in detail for its applicability. Helpful in this procedure is the gathering of any prior art that is dated before the patent filing. Prior art must not necessarily be a published paper, but can be a citation, a picture, a slide, etc. If the reader knows of any early work in the field of rights expression languages, please write to the ODRL interest list.

Current and future work of the ODRL initiative

In the past year, the ODRL Initiative has established the ODRL International Advisory Board, which includes members from research and industry and guides the ODRL Initiative in long-term strategy and governs the ODRL policies and procedures.

Intensive work on the further development of the ODRL language model is currently being addressed. A comprehensive language requirements document has been published by the ODRL Version 2.0 working group. A first draft of the new Version 2.0 data model (cf. figure 1 page) has been released for discussion. After the final review, several encodings e.g. XML, RDF, are to follow. The ODRL Version 2.0 data model will meet future needs by having the expressiveness for multi-sided contracts comprising rights *and* duties, barters, service level agreements (SLAs), downstream (next) rights, tickets, reuse of existing, related standards etc., and at the same time being simple and easy to use.

The application areas of ODRL are numerous and so are the various ways it is used. Thus, creating application or domain specific profiles of ODRL is the logical and necessary future step. Three weeks ago, the first official ODRL Profile Specification for encoding the Creative Commons licenses in ODRL was published. The ODRL Initiative looks forward to working with other communities in developing new profiles to capture their requirements for content licensing and sharing. Mechanisms to achieve this are via new joint ODRL Working Groups and more formal liaisons with existing standards and community sectors groups.



Bottom line

Workshop participation, the contributions, and the given talks illustrate the strong industry and research interest in the field of rights expression languages and DRM implementations. Furthermore, it is has made clear that

the application areas of DRM and rights expression languages are not restricted to e.g. digital music distribution anymore. The main topics of the workshop were interoperability and standardization, as well as integration of related technologies, which will also continue to be the focus of the ODRL Initiative.

Sources

- Buhse, Willms: The Open Mobile Alliance releases OMA DRM 2.0 — moving from OMA 1.0 onwards. The INDICARE Monitor Vol. 1, No 3, August 2004; http://www.indicare.org/tiki-read_article.php?articleId=37
- The CoreMedia website is available at http://www.coremedia.com/
- Coremedia (2005): CoreMedia first to combine mobile OMA DRM with Microsoft DRM – Delivering cross platform interoperability for PC; http://www.coremedia.com/coremedia.aspx/company/presse/archiv/2005/20050721-drm-microsoft/language=en/id=93252/20050721-drm-microsoft.html
- Guth, Susanne, Iannella Renato: Critical review of MPEG LA software patent claims. INDICARE Monitor, Vol 2, No.2, March 2005; http://www.indicare.org/tiki-print_article.php?articleId=90
- The MPEG LA website is available at http://www.mpegla.com
- The ODRL Profile Specification for Creative Commons is available at http://odrl.net/Profiles/CC/SPEC.html
- The ODRL website is available at http://odrl.net
- The ODRL Workshop 2005 website is available at http://odrl.net/workshop2005
- The Open Mobile Alliance (OMA), La Jolla, California: http://www.openmobilealliance.org
- The NETWORKED AUDIOVISUAL SYSTEMS AND HOME PLATFORMS (NAVSHP) website is available at http://www.rose.es/navshp.

About the authors

Susanne Guth received a diploma degree in Information Systems and a doctoral degree in social and economic sciences.. She wrote her doctoral thesis in the field of contract and rights management for digital goods. Susanne Guth is a private, active member of the ODRL Initiative, leading the development of ODRL Version 2.0 and works as DRM senior specialist for the German mobile network operator O2. Contact: susanne@odrl.net

Renato Iannella is a Program Leader at National ICT Australia (NICTA). Renato has extensive experience in the development and standardisation of Internet, Web, and Mobile technologies and was a former member of the World Wide Web Consortium (W3C) Advisory Board. Renato also is an Adjunct Associate Professor at the University of Queensland, Visiting Associate Professor at the University of Hong Kong. Contact: renato@odrl.net.

Carlos Serrão has two academic degrees (BSc and MSc) from Instituto Superior de Ciências do Trabalho e da Empresa (ISCTE). He is currently a lecturer at ISCTE, teaching subjects related to Information Security, Information Systems Development and Management, and Project Management. Carlos Serrão is currently preparing his PhD in the DRM area. Contact: carlos.serrao@adetti.iscte.pt

Status: first posted 28/07/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=126

Editorial of INDICARE Monitor Vol. 2, No 6, 26 August 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: An INDICARE-interview with *Arnoud de Kemp* about DRM in scientific publishing marks the start of this issue; six contributions related to the entertainment business follow: the fight against "piracy" is dealt with in an INDICARE-interview with *Tim Kuik* (BREIN - Beschermning Rechten Entertainment Industrie Nederland), the successful fight of consumers for their rights is exemplified by a decision of the Cour d' Appel de Paris (Mulholland case), and opinions of "Indies" about DRM are collected in a third article. Further articles tackle developments at the level of DRM technology providers: first, agreements of Microsoft with Philips, Nokia and CoreMedia are analysed, second, lessons are drawn from the recent DRM Strategies Conference held in New York, and third the chances of DMP (Digital Media Project) to establish an open DRM standard are assessed. Finally, *Nicholas Bentley* presents a new conceptual approach how to best regulate the distribution of copyrighted works in a digital environment.

Keywords: editorial – INDICARE

About this issue

DRM in scientific publishing

The interview by *Ulrich Riehm* with *Arnoud de Kemp,* responsible till 2004 for the development of new media and electronic publishing at scientific Springer-Verlag, reveals fundamental differences between scientific publishing and entertainment the entertainment business: The circulation of scientific publications is orders of magnitude below the one of music and films, royalties to authors appear to be more the exception than the rule, and scientific publishers don't strive to control the behaviour of end-users, as scientists maintain a tradition of free exchange of information and dislike monitoring how they use information.

In addition, scientific publishers have in most cases to do with institutional customers and are not able to control the end-users directly. Although DRM systems still play a minor role in scientific publishing, they are not absent – think e.g. of document delivery services. A rather optimistic statement of de Kemp is that "scientific literature for the end-user is in most cases in principle freely accessible". *Peter Suber*, OA advocate, has already disagreed about it in an online-comment at INDICARE.

Fight against piracy, fight for consumer rights, opinions of Indies

The interview by *Margreet Groenenboom* with *Tim Kuik*, director of BREIN, an organisation acting for the entertainment industries in cases of assumed copyright infringements, centres around copyright infringement, circumvention of technological protection measures, and the distribution of circumvention devices. It is good to hear that "BREIN only acts when one is able to speak of an activity of commercial significance…".

The next article deals with a particular case in which a consumer, supported by consumer organization Que Choisir in France filed a lawsuit against Universal Pictures Video France and others. Mr. P. had bought a DVD realizing afterwards that he could not make a private copy of it due to technical protection measures in place. In first instance he lost, while the Cour d' Appel de Paris now repealed the decision of the first instance. *Natali Helberger* presents the main arguments of the decision and elaborates on its groundbreaking implications.

Philipp Bohn has interviewed protagonists of the independent music scene (Indies), which does not only mean independent labels, but also content aggregators, technical service providers and distributors. Corresponding to the image of "Indies" the answers show the sympathy of Indies for consumer concerns and their antipathy to strong technical protection measures - more likely to accept forensic DRM. However, the Independents sometimes depend on powerful distributors who decide.

Technology providers' strategies and Microsoft's gravity

Philipp Bohn writes in his second article for this issue about agreements between Microsoft and three companies (CoreMedia, Nokia, and Philips). CoreMedia announced to provide interoperability between the Open Mobile Alliance's (OMA) DRM and Microsoft's DRM system; Nokia announced that its music-oriented handsets will support Microsoft's DRM system, and Philips will use Microsoft in its consumer electronic products (Nexperia family etc.). These agreements help to build DRM-bridges between the PC world, the mobile segment and consumer electronics. As the common denominator of these bridges is Microsoft DRM, these agreements are likely to strengthen the position of this player.

Thorsten Wichmann, who presented results of the INDICARE consumer survey at the Jupiter DRM Strategies Conference held last month in New York, also watched out for developments at the level of DRM technology providers. He found important indications for Microsoft's growing importance in the DRM business: uncertainties in IP matters not yet settled favour the choice of less risky Microsoft DRM technology paving the way to become a *de facto* standard. The strong position of Microsoft in the enterprise DRM sector is another indicator of Microsoft gaining strength as developments in this sector will also have consequences for consumer markets. The gravity of Microsoft seems palpable, the question if this roads to interoperability is the best and if it is inevitable may however be doubted.

Ernö Jeges and *Kristóf Kerényi* have analysed an alternative approach to DRM standardisation, namely the Digital Media Project's "Interoperable DRM Platform" (IDP) aimed to become an open standard. The authors conclude that market forces won't favour this approach, and they opt instead for governmental enforcement of interoperable standards.

A new approach between OA and DOI

Finally *Nicholas Bentley* introduces the "contributions model" and the Rights Office System, a new approach to manage rights in a digital environment, and compares it to existing schemes based on DRMS, CC and levies. The basic conceptual assumption is that all intellectual works can be described in terms of "contributions", part of which mean the sources used to produce new intellectual property, others refer to actions and transactions once the work is publicly available, such as payment, review, criticism, recognition, quotations, citations, and recommendation. The enforcement of intellectual property as a private good is abandoned and the character of intellectual property as a public good in the digital environment is stressed. Instead of a mono-directional exploitation chain, the model is relying on an exchange of rights to intellectual works. The Rights Office system is the envisaged infrastructure to mange the exchange of rights. Each contribution, no matter if it is an intellectual or a monetary contribution, is determined by two, unique, persistent, identifiers. In my view this model is located somewhere in the expense between OA and DOI. What still puzzles me most is how incentives to pay can effectively be implemented in the model. As the approach is not easy to resume in one paragraph, please take a closer look yourself and don't hesitate to discuss it at the INDICARE site.

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 29/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=137

Science can't accept technical barriers of content use!

What matters in scientific publishing are licenses, contracts, and laws

By: Arnoud de Kemp, digilibri, Heidelberg, Germany

INDICARE-Interview by Ulrich Riehm, ITAS, Karlsruhe, Germany. The interview explores the special situation of scientific publishers with respect to the application of DRM systems. Arnoud de Kemp is convinced that scientific publishing is subject to completely different conditions than those prevailing in the entertainment sector. Among the special characteristics are a tradition of free exchange of information among scientists and unlimited access to full-text databases ruled by consortium contracts. Extensive controls and restrictions of use are not likely to be accepted by scientists and they are also unnecessary as long as legal and contractual regulations work fine.

Keywords: interview – consumer expectations, DRMS, scientific publishing, stakeholders, DRM users

Arnoud de Kemp *was the marketing and sales director and deputy member of the board of the scientific Springer-Verlag from 1984 to 2004. Apart from worldwide sales and marketing, he was responsible for the development of new media and electronic publishing ("SpringerLink"). He was a member of the Executive Board of the International Association of Scientific, Technical, and Medical Publishers (STM), was from its very start active in the International DOI Foundation, a long-time Director of the International Electronic Publishing Research Centre (IEPRC), past President of the Deutsche Gesellschaft für Informationswissenschaft und –praxis (DGD, now DGI) and now Chairman of the Electronic Publishing Working Group (AKEP) in the Börsenverein des Deutschen Buchhandels (Association of German Publishers and Booksellers), with lots of other activities going on.*

Since 2004, he and his associate Ingrid Maria Spakler have been building up the digital agency and publisher "digilibri" in Heidelberg, which sees itself as an intermediary between suppliers and purchasers and which is using advanced database and security technology, especially access rights and digital watermarking. digilibri just opened its new website, a media database and an online Asset Management System with a special programme "digilibri-pro" for publishers and other organisations that would like to manage, catalogue and present their digital assets, in particular images with texts. digilibri turns digital objects on the fly into electronic publications by assigning a Digital Object Identifier and registering the electronic publication in a central internet register for permanent identification, citation and retrieval.

Arnoud de Kemp is acknowledged as one of the pioneering experts in the international scientific and professional publishing landscape. With his new company, digilibri, he is also in a position to argue from the point of view of an advanced user of DRM. Contact: dekemp@digilibri.de.

INDICARE: Mr. de Kemp, there is a lot of talk about Digital Rights Management (DRM). Our impression is that scientific publishing is largely unaware of this. Is that correct?

A. de Kemp: What's in a name? Publishers use DRM, but they call it something different. Maybe, because they organised themselves long before DRM became a well-known expression. Henceforth DRM is far more used by science and professional publishers as well as by learned societies than is generally perceived.

INDICARE: What is your underlying conception of DRM?

A. de Kemp: My overall simple definition of DRM is: DRM is nothing else but electronic

or digital registration and control of the access to media, both databases and specific content. This might start with the registration of subscriptions to printed journals in large computer systems of subscription agencies and publishers, go through the exploitation and administration of access to electronic journals through journal agencies or in electronic library collections, and go on with electronic watermarks in all kinds of documents, e.g. in audio books. This is a very broad area. The amazing thing however is that, apart from watermarking, publishers, libraries and journal agencies have been using such systems for much longer than the term "DRM" has been in fashion. In the area of scientific and professional publishing, the term DRM has not been and is hardly being used at all. People that are involved in system development, database management, telecommunication etc. of course use a different language, but they are not publishers.

In a more narrowly scientific definition, one would stress cryptographic encoding, digital identification and the regulation of use. I regard the registration of access and the metering of use up to billing as important and because there is much more money involved, the music publishers and entertainment companies exploiting their content commercially have been far more active.

INDICARE: Where do you see the difference between the entertainment industry which has strongly pushed the debate on DRM and the scientific publishing domain?

A. de Kemp: There is a whole series of differences. The most important is that in science there is a long tradition of free exchange of research results. Scientists go to conferences and present papers, present and defend their issues in poster sessions. This may result in articles that are offered for publication. Most of the material comes in unsolicited, some material is written on invitation (invited papers). For journal articles, there are no royalties involved. Secondly, you have to realise that there are only a few very large scientific publishers. The majority are small companies, university publishers and learned societies. There is little cooperation and limited standardisation going on between publishers, except for SGML and DOI. Most of the standardisation, that publishers use, comes from industries like Adobe (with PDF), database developers and network companies. Broadcasting of music and television is a completely different business than that of the scientific publishers. A good scientific journal may have a printing of up to 3 to 4,000 copies and that's it. Thirdly, we have completely different distribution channels. We sell our content, in particular journals, by subscription through bookshops and specialised subscription agencies, primarily to libraries and institutions. Practically all journals now also exist in electronic form. It is still common to sell a combination of a printed title and its electronic version. Libraries can licence for one title, a series of titles or entire full-text databases and their users then have unlimited access and can download text documents. In other words, we seem to have a straightforward DRM environment in scientific publishing, distribution and dissemination. There are services run by publishers or learned societies or aggregators, that are based on metered downloads, these however are mostly for bibliographic and factual databases: abstracts, tables of contents, chemical structures, chemical reactions, patents, news, business information, and stock market quotations.

I'd like to mention one more specific feature of the entertainment business: the prices for CDs and videos are kept artificially high by the entertainment industry. The proliferation of self-burned CDs or DVDs may thus be seen as a kind of consumer protest.

The music industry has to pay royalties to composers, song writers, musicians, conductors, studios etc. It is a far more complex business. In our world, the use of photocopiers is metered and a little fee per copy made is then paid to the central reproduction right organisation (RRO), which pays publishers and registered authors according to certain schemes. Publishers mostly pay royalties only to book authors, but with many works in science, which consist of individual contributions, not even that is the case. The publisher makes the investment, takes the risk, guarantees continuity and promises to make the content publicly known. The authors / con-

tributors get the reward of being published and hopefully cited. For a lot of journal publications the author has to pay a page charge to support the publisher: In most cases these publishers are societies and the payment is to keep the price of the publication low, especially for members of the society. The "Open Access" initiatives support that authors and their institutions pay enough money to make the publication free to anyone.

INDICARE: What is actually happening at publishers with respect to the introduction of DRM in the stricter sense?

A. de Kemp: Next to nothing is happening, as in the world of publishing, people feel that everything is already taken care of. Through the consortium licenses and copyright laws, there is the possibility for unlimited use of scientific literature. Students can log in from home and access literature from the databases that are licensed by the university libraries. In this way, scientific literature for the end-user is in most cases in principle freely accessible. There is little inclination to copy and disseminate scientific articles as an alternative.

During the past two years, there has been a hefty debate on the reform of German copyright law, under which professors, teachers, students and workgroups are to be allowed to copy parts of works and store these. There was a great fear among publishers that through this, entire journals, journals or works of reference would "leak". In my opinion, this is largely unfounded since digital literature is mostly already "free" in an organised way. It is different however with books, especially textbooks, where we still have very little experience as only few are available in electronic format.

INDICARE: Isn't there the fear that a scientist could download an article from Elsevier's Science Direct or SpringerLink and, for instance, make 10 copies which he passes on to his colleagues?

A. de Kemp: He has access to his own article and he is allowed to do that. For research and teaching purposes such practices are permitted. But it does not work that way. He will send a mail with an attachment or with a link. Still, lots of scientists order offprints or original PDFs from their publishers for documentation purposes in the funding and approval process and for exchange with colleagues.

Most publishers nowadays allow authors to store a copy of their article on their own server if at least a link to the original and formal publication by the publisher is made.

INDICARE: And there are no forces in the publishing world that are now saying, "we will no longer allow that, since in DRM we have the technical means to prevent it"?

A. de Kemp: No. As long as it is covered by licenses, contracts and laws, it is not seen as a major problem. We had that debate in the course of the reform of the German copyright law and the implementation of the law in practice certainly still needs close monitoring to prevent ill use. But in general, in the scientific publishing world the tendency is that current organisation and regulation is adequate. What we do not want, is mass copying by libraries, which then provide large-scale document delivery services in unfair competition with publishers of all kinds, for profit or not for profit.

Who should control individual use? That is the crucial question. The publishers are unable to control individual use at universities since there is only one central point of access. Publishers and their agents provide statistics on the general use to the universities and are happy, in most cases, that the literature offered this way, is better used than ever before. Reading rooms in university libraries are full nowadays.

We have had extensive discussions on this in STM circles, the International Association of Science, Technical, and Medical Publishers. Everything attempted in this direction in the past, watermarks, digital envelopes which have to be opened with codes received previously or afterwards, did not meet with acceptance. People don't want it. Scientists and students want information without technical barriers.

INDICARE: No further restrictions? No stipulations that this document may only be

used on a single computer or, for instance, be printed once only?

A. de Kemp: No, no further restrictions. Anything more is not feasible to control. If one has institutional license agreements or consortium contracts with large data centres and universities, then access control is only possible by means of a general IP address. We cannot determine who is behind it. That's a problem. It is not like in P2P or B2B where there is a direct relationship between supplier and consumer. Our route is from a supplier to a large grey cloud called university. We are unable to ascertain whether this means 10 or 200 institutes or 2,000 or 10,000 students and we are also unable to organise transparency in this respect, apart from a description in the contract.

INDICARE: Do you mean that the effort to control individual transactions would be too great?

A. de Kemp: No, systems from publishers and agents would not be able to do it. Universities and their libraries don't work with access control. Everything is open. It is different in the industry, which also licenses our content. They don't wish anyone from the outside to know who is using which information. Industries may have very detailed internal costing or profit centres. But that is their issue, not ours. They don't wish transparency on which articles and documents are being used. That is by no means such a sensitive subject in the distribution of music as it is in science and research.

About barriers, we have been confronted directly with this problem when building up "digilibri". We supply pictures, high-quality photos, copies of antique documents, high resolution images of original paintings with lots of descriptive text. For each image the rights situation is documented in a very flexible way. From the very beginning we considered to work with DRM as we needed to prevent this sensible material from unwanted commercial exploitation. This starts with registration. We present three look-up formats: thumbnails a preview and a very large preview, all in a low resolution, but enough for a computer screen. We add intelligent watermarks. Each document to be found in our media database in each format is now protected by a visible "digilibri" watermark. Only registered users are allowed to see the large preview. Once a registered purchaser interested in the image has clarified all issues, related to use and exploitation, the image is released as a download or submitted on a DVD, which we think is the better way to ship high-resolution material anyhow.

However, we soon noticed, during the tests we conducted, that the acceptance of visible watermarks among artists, photographers, illustrators who see their own works in the database with a watermark is rather low down to negative. At the moment we're therefore thinking of using invisible or more transparent watermarks.

INDICARE: Hence you would be taking a direction that specialist calls forensic DRM.

A. de Kemp: Yes, of course we are thinking in this direction, although there are also problems with forensic DRM.

INDICARE: What would be the alternative?

A. de Kemp: The open route using contracts. We will conclude framework contracts with editors, image agencies, designers etc. and give them open access to our material in a special catalogue, controlled by their IP address, user name and password. We provide user rights by contract in the conventional manner (printed, stamped, sent by fax with signatures etc.) and the material provided is given no further protection.

INDICARE: Besides those that you have already mentioned, are there any other barriers to the introduction of DRM in publishing houses? For instance, is DRM too expensive, not sufficiently reliable, or inadequately standardised?

A. de Kemp: To me, the last point seems to be the main problem. There are still no standards for reliable encryption in the dissemination of scientific documents. The user does not appreciate being restricted by all kinds of technologies.

At Springer, we used to have never-ending tests with CD-ROMS, trying to encrypt them. Most technologies were obsolete from the

beginning or soon became obsolete. I realize that there are more advanced technologies.

INDICARE: Isn't Adobe-Acrobat already the standard?

A. de Kemp: Yes, it is currently the best encryption for documents that we can imagine. Fantastic. It comes along with all PCs and Macintosh computers as an OEM product and the Acrobat Reader can be freely used. That is why it has been so successfully established.

By the way, there is the DocuRights system by the Aries Company that builds up on PDF. It is being tested and partly already used by a number of STM publishers. At Springer, we were also investigating it, but I don't know if Springer made the decision to apply the system. DocuRights wraps the document in a secure container and protects it regardless of its physical location in the Internet. During my time at Springer we actually came to the conclusion that this was an interesting technique, but not necessary.

INDICARE: Let's have a look at other actors involved in the exploitation of scientific content, e.g. the collecting societies. Some argue, that collecting societies might become obsolete due to DRM systems, because collective rights management and compensation schemes could now be replaced with more equitable, individual use-based billing. What do you think about this?

A. de Kemp: The collecting societies were created to collect and administer fees, charges for copiers, fax machines, DVD burners, scanners, blank media etc. Somebody has to collect, administer and distribute these dues. And that can practically only be a centralised organisation.

The alternative model is to concentrate on content and attempt to measure it. That is extremely complex and difficult to achieve, since organisations like the collecting society "VG Wort" have a legal basis and too many parties in the information sector are involved.

In the medium term, I would hope for a shift in the tasks of the collecting societies. For instance, combining Digital Object Identifiers (DOI) and DRM systems, one could establish a kind of usage counter and use this at least for detailed metering, in the long term even for a better distribution of the money to publishers and authors. The collecting societies would no longer be superfluous, since they could be responsible for the business of accounting and billing. This would not be limited to texts and images. The DOI would also be a perfect facilitator in other sectors like digital music, audible books, download platforms in general.

INDICARE: How do you view the relationship of scientific publishers to the open access movement?

A. de Kemp: As I have said before. "Open Access" wishes to make all published material free of charge. In their view, libraries and scientists stand on one side and the publishers and their helpers on the other. In principle however, the publishers should not be against "Open Access". If the money that the libraries currently pay to publishers for the use of the publications is re-allocated by the funding agencies and similar organisations, to finance the publishing process and dissemination of electronic publications, we as publishers should be happy as life will be easier. Springer very quickly presented "Open Choice" with good arguments: we don't care who pays, but whoever pays, can determine the rules of use. The "Open Access" movement is a real anti-DRM movement. The danger of "Open Access" is that relevant scientific literature becomes grey literature and there are big issues like originality, exploitation of the results described all the way up to patent application, that are not addressed at all.

INDICARE: To close, a question about the more structural mid-term changes. How do you see the functional and structural changes in scientific publishing?

A. de Kemp: Positively! By consortium contracts with universities and entire countries, scientific context is accessible everywhere. CrossRef will continue to spread its influence and support linking and hopefully better access to full text as Scholar Google is currently attempting. In the past, publications were "hidden" in large or small university libraries and not accessible. Finding the way

was not always easy. Bibliographic databases have been around for a long time, but that is a very narrow access. Now the material is accessible around the clock on the Internet. That's a fantastic development.

But I have a different worry. The worry's called Google and I have a great fear that we are being "googlified". The great simplicity and the enormous quantitative search results that Google produces are being seen uncritically. This might result in a tendency to no longer use documents, articles and books, but to solve all our information problems using Google. There, information is not really indexed deeply enough and the algorithms behind the ranking are unclear. "Googlification" should create great concern for everybody in the information as well as education sector, including parents of children.

The time will come that the majority of library holdings is available digitally. There are initiatives everywhere, triggered or accelerated by announcements from Google and Amazon to digitize whole libraries or make whole publisher catalogues readable (Inside the Book). The French National Library, the European Library, led by the Royal Library in the Hague, large university centres like Göttingen in Germany or Cornell in the US, all have retro-digitisation projects. The Gutenberg project is also a project to digitise out-of-print books. Soon, we will have the whole world in our hands.

INDICARE: Thank you very much for this interview.

Sources

Important institutions and projects mentioned in the interview:

- Arbeitskreis Elektronisches Publizieren des Börsenvereins des Deutschen Buchhandels http://www.akep.de
- Aries Systems Corporation http://www.kfinder.com/newweb/home.html
- BnF – Bibliothèque nationale de France – Le débat autour des projets de numérisation http://www.bnf.fr/pages/zNavigat/frame/dernmin.htm?ancre=com_google.htm
- Cornell University Library Digital Collections http://cdl.library.cornell.edu/
- CrossRef (Publishers International Linking Association – PILA) http://www.crossref.org/
- DGI – Deutsche Gesellschaft für Informationswissenschaft und Informationspraxis http://www.dgd.de/
- Digilibri http://www.digilibri.com/
- DocuRights http://www.docurights.com/
- DOI – Digital Object Identifier System http://www.doi.org/
- Elsevier ScienceDirect http://www.sciencedirect.com/
- GDZ – Göttinger Digitalisierungszentrum – Center for Retrospective Digitization, Göttingen State and University Library http://gdz.sub.uni-goettingen.de/en/index.html
- Google Print http://print.google.com/
- Google Scholar http://scholar.google.com/
- IEPRC – International Electronic Publishing Research Centre http://www.ieprc.org/
- The European Library: http://www.theeuropeanlibrary.org/portal/index.htm
- Koninklijke Bibliotheek – Royal Library Den Haag – http://www.kb.nl/
- Project Gutenberg http://www.promo.net/pg/
- Projekt Gutenberg http://gutenberg.spiegel.de/
- Springer-Verlag http://www.springeronline.com/
- STM – International Association of Scientific, Technical, and Medical Publishers http://www.stm-assoc.org/

Status: first posted 09/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=129

Protecting the entertainment industry against commercial piracy – About arguments and actions of BREIN

By: Tim Kuik, BREIN, Hoofddorp, the Netherlands

INDICARE-Interview by Margreet Groenenboom, IViR Amsterdam, the Netherlands with Tim Kuik, director of BREIN (Bescherming Rechten Entertainment Industrie Nederland). Circumvention of Technical Protection Measures (TPM) as well as distribution of circumvention devices are not allowed by article 29a of the Dutch Copyright Act and article 19 of the Dutch Performers and Phonograms Act. One of the organisations that act for several copyright owners and neighbouring right owners when piracy of their works occurs is BREIN. In this interview the director of BREIN, Tim Kuik, shares insights about rationale and practice of his organisation.

Keywords: interview – content industries, copyright law, piracy, private copy, technical protection measures – The Netherlands

About Tim Kuik and BREIN: *Mr. Kuik is the director of BREIN. BREIN stands for the Protection of the Rights of the Entertainment Industry of the Netherlands, and as a result, BREIN fights piracy of copyrighted works of the members of BREIN. Piracy is understood by BREIN as the unauthorised copying and distribution of copyright protected works. These works can be music, movies, games or interactive software. BREIN is not limited to any one type of works but aims to fight large scale commercial copyright piracy of all works for its members; offline (bootleg or counterfeit CD or DVD) and online (illegally uploading music) – no matter what the subject is.*

INDICARE: Mr. Kuik, when were you concerned with Digital Rights Management (DRM) for the first time?

T. Kuik: From the 1980's on, I have been concerned with DRM as a copyright expert for filmstudios. That was before BREIN existed (BREIN was established in 1998). A case I was involved in concerned the protection of pay-TV smartcard technology in Ireland. The smartcard was hacked and the problem was that if you reveal how the smartcards works in a civil or criminal law suit, you give away the blueprint and the security of the smartcard becomes worthless. There was a clear need for *sui generis* legislation prohibiting circumvention of the technological protection device, the smartcard, without giving away how the technology works. This legislation needed to prohibit not only circumvention but also distribution of circumvention devices. With the current legislation on the circumvention of TPMs, this *sui generis* legislation has been realised.

This issue also plays an important role for DRM systems relying on TPM. These can be hacked, see for example the DeCSS case some years ago (This programme is capable of decrypting content on a DVD that has been encrypted by using the Content Scrambling System). From the 1980's on, I promoted the use of DRM systems but it took a lot of development to make them acceptable for consumers, because they were either cumbersome and expensive or cheap but easy to hack.

INDICARE: What is your general view of DRM?

T. Kuik: In the view of BREIN, copyright owners should have the possibility to decide themselves how they want to exploit their work. Do they wish to exploit the work on the Internet or not? If they want to use digital exploitation on the Internet, they should have the possibility to either use a DRM system (and as a consequence to decide under which conditions they want to license the content) or to make available free downloads from their websites.

A DRM system can be protected by TPM. As you know, circumvention of TPM and distribution of circumvention devices is not

allowed by the articles 29a Dutch Copyright Act and 19 Dutch Performers and Phonograms Act. So if copyright owners do decide to use TPM, and someone circumvents this protection measure, or someone distributes circumvention devices for a commercial purpose, BREIN takes action and sues the alleged infringer.

I think that when people talk in general about the definition of DRM, a distinction can be made. On the one hand there is simple DRM which aims at copy protection, and on the other hand there is more detailed DRM which uses watermarking or fingerprinting to distinguish individual works and/or makes it possible to charge for individual use.

When talking about download services such as Apple's iTunes, an issue that will become much more important in the future is the interoperability of services. When services become interoperable, this is likely to lead to a greater acceptance rate of DRM systems by consumers. In my view, what is also important for consumers is transparency. When copyright owners do decide to protect their CD in a way that consumers cannot make a private copy of the CD any more, this should be stated on the CD. If it would not be stated on the CD, this would not be fair to consumers because they are used to being able to make a private copy.

INDICARE: The articles 29a and 19 already mentioned became effective in 2004. Have these articles already formed the basis of a prosecution initiated by BREIN in the Netherlands?

T. Kuik: Interestingly enough, on 21 July 2005 the District Court in Rotterdam gave his judgement on the first case initiated by BREIN involving the commercial distribution of circumvention devices. BREIN obtained an injunction against the company Teledirekt which distributed circumvention devices that have been ruled unlawful in the United States. The case concerned the programs DVD X copy Gold, DVD X copy Platinum and DVD Xpress. With these programs it is possible to circumvent the CSS on a DVD. It was advertised by Teledirekt in their brochure that this programme "is the most effective programme to make a copy of a DVD" and "it is able to handle all kinds of protection on DVDs". Moreover, Teledirekt's direct mail mentioned "Copy also protected DVD movies. Circumvents all protection measures". Teledirekt suggested that it should be possible to make a back up copy for consumers of DVDs and that their programme DVD X copy would enable this. The judge ruled though that the programme can be considered as a circumvention device and distribution of those devices is not allowed on the grounds of 29a of the Dutch Copyright Act.

INDICARE: This case concerned the distribution of circumvention devices. Are there also lawsuits expected on the circumvention of TPM?

T. Kuik: Of course, when cases arise, these will be pursued by BREIN with civil enforcement actions. At the moment, what we see occurring in the Netherlands, is the distribution of circumvention devices and methods instead of the hacking of technological protection itself.

INDICARE: You said earlier that every kind of protection ultimately is hackable, do you think TPMs are efficient enough to protect copyrighted works?

T. Kuik: Yes, in my opinion they suffice for protecting works although there always is the possibility that a TPM can be circumvented. That is why legislation prohibiting circumvention and distribution of circumvention is required.

INDICARE: Recently the Enforcement Directive (Directive 2004) was adopted. Will this Directive influence the current possibilities for enforcement of copyright (thinking for example of article 8 which encompasses the right to request information in the context of proceedings concerning an infringement of an intellectual property right)?

T. Kuik: This Directive will certainly clarify the current situation with regard to what internet providers should do when a copyright infringement occurs. For instance, BREIN sued several internet providers because they refused to give the name and

address data of certain alleged infringing users of peer-to-peer networks. The judge ruled that BREIN is entitled to ask the providers for this data and that the providers should consider supplying those to BREIN. In the circumstances of the particular case the judge denied BREIN's claim, in short because use was made of an American company to collect IP addresses and download data.

INDICARE: The making of a private copy is allowed on the basis of article 16b and 16c of the Dutch Copyright Act. Imagine someone circumvents a TPM for making a private copy. What is your opinion about this?

T. Kuik: First, I would like to mention that in principle the private copying exception is not a right for consumers but an exception to the exclusive right of copyright owners. When it is possible to make a private copy, then there is no problem. Again, transparency as to whether it is possible to make a private copy, is very important. In my opinion, circumvention to realise a private copy, should not be allowed. The risk exists, that everyone will say that they are making a copy only for private use. Where should you draw the line in that case? It is very hard to make a proper distinction between the honest consumer who makes a private copy indeed intended for own personal use or study and the dishonest consumer.

INDICARE: In Italy it is also not allowed to circumvent a TPM, but in case this occurs for the purpose of making a private copy, the punishment will be less severe than when circumventing occurs for commercial purposes. Should this example be followed in the Netherlands?

T. Kuik: In civil law suits it is the judge who decides on the punishment. Probably he will take into account that circumvention took place to make a private copy. I think this case is hypothetical because if indeed the copy was made as a private copy, no one will find out about it. Only in the circumstance that the maker of a private copy takes another action, for instance placing instructions on how to circumvent a certain device on the internet, his circumvention becomes public. At that moment, his behaviour can not be seen merely as the making of a private copy anymore, he does something more and will be liable accordingly. BREIN only acts when one is able to speak of an activity of commercial significance; the making of a private copy would not qualify, but offering circumvention devices or placing information on a website on how to circumvent a TPM certainly does!

INDICARE: Who should in your opinion be liable for guaranteeing the protection of the consumer: the consumer, judge, legislator or consumer organisations?

T. Kuik: The legislator is the one who is responsible for balancing the rights of rightholders and consumers. The next step, clarifying the law, will be the responsibility of the judge. Consumer organisations also play an important role because they are able to present consumer interests to rightholders, for instance about making use of the exceptions that are incorporated in the Copyright Act. I believe that it all comes down to what the consumer wants because the end goal of the rightholder is to get his product to the consumer.

INDICARE: What will in your opinion be the future of legal download services versus the peer-to-peer networks?

T. Kuik: At the moment the market share of legal download services is growing rapidly and even legal file sharing of music is in development, for instance Snocap by Shawn Fanning of Napster fame. When downloading music, consumers will take the easiest and fastest way which guarantees the best music quality. Peer-to-peer services do not guarantee music quality or even that you find what you asked for and, moreover, there is the risk of not only downloading the music file but also spyware. When there are more legal download services people will use these more and more because they know it is good quality music and more important, the one offering the music can be identified and addressed.

INDICARE: Mr Kuik, thank you very much for this interview!

Sources

- BREIN website http://www.anti-piracy.nl
- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights; online available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf
- Judgment District court Rotterdam 21 July 2005, BREIN / Directwarehouse BV (Teledirekt), KG ZA 05-527 and KG ZA 05-567

Status: first posted 25/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=131

Not so silly after all – new hope for private copying

By: Natali Helberger, IViR, Amsterdam, The Netherlands

Abstract: The decision of the French court in Paris in the so-called Mulholland case has left a sour after-taste since. Could it be true that the private copying exception, a long standing tradition in many national copyright laws, was in fact not much more than a toothless paper tiger? When we reported about this case we expressed our disbelief that this should have been the end of the private copying exception. And indeed, as the Court of Appeals has recently decided, the tiger may be made of paper, but it still has its teeth.

Keywords: legal analysis – consumer expectations, consumer law, private copy, court decision, EUCD, film industry, technical protection measures – France

Introduction

In an earlier article (Helberger 2004) we reported about the "Mulholland Drive" case – a case that was bad news for private copying. It was the case of Mr Stéphane P. in France who had bought the DVD of Mulholland Drive. Later, he had to realize that technical protection measures in place prevented him from making a copy of this film for his parents. Together with the French consumer organization L'Union fédérale des consommateurs "Que Choisir" (UFC) he started proceedings before the Tribunal de grande instance de Paris 3ème chamber (Tribunal Paris 2004). And he lost.

The Paris court dismissed the plaint by saying that the private copying exception in French copyright law was not a right of consumers and, hence of no or little significance for consumers who complain about technical anti-copying protection. The court, moreover, cast some doubt on the compatibility of the private copying exception with the so-called three step test (in more detail see below) in the case of digital copies. The Paris court held that the interest of distributors in selling copies of DVDs was an act of normal exploitation, based on a legitimate interest to recoup the investments made. The pursuance of this interest may not suffer from the possibilities technology offers, namely to make a private copy, so said the court of first instance. But the last word in this matter was not yet spoken.

The case went into appeal and was decided in April of this year (Court of Appeals, Paris 2005). The Court of Appeals repealed the decision of the first instance, and it became clear that it disagreed with most points. The decision is enlightening in many respects. This article will report some of them.

Main arguments of the Court of Appeals

Private copying exception not at the disposal of rights holders

The Court of Appeals answered one nagging question that many readers of the first decision had: even if the private copying exception is not a "right", can this mean that rights holders are free to simply ignore it? The de-

cision from April made unmistakably clear that the private copying exception, even if it is not a "right" but "just" an exception, is still law. The Court of Appeals said that it is up to the legislator to formulate limitations to the private copying exception or the modalities of limiting the private copying exception ("cette exception légale ne peut être limitée qu' aux conditions précisées par les textes"). The private copying exception is not per se at the disposal of private parties, such as DVD producers and distributors; they still must abide by the law even if consumers have no corresponding right. The court said explicitly that the complete blocking of any possibilities of making private copies was an impermissible behaviour under French copyright law ("comportement fautif de sociétés qui ont 'verrouillé' totalement par des moyens techniques le DVD en cause").

Making the use of TPM subject to restrictions is a task of the legislator

The Court of Appeals refrained from specifying under which conditions the use of technological measures would not conflict with the private copying exception. The Court of Appeals found that Article 6 (4) of the European Copyright Directive (EUCD 2001), i.e. the provision that addresses the relationship between technological protection measures and exceptions in copyright law, did not formulate a principal obligation for rights holders to observe the private copying exception or any other exception in copyright law. Neither was it up to courts to replace the legislator in this matter determining how technological protection measures should look like in order to be in conformity with copyright law. The court also refrained from drawing any conclusions concerning the interesting question of whether technological measures that do not respect existing boundaries in copyright law still deserve the protection of the so called "anti-circumvention rules". The decision of the Court of Appeals confirms, however, once more that the rules on the legal protection of technological measures in copyright law are still in many respects flawed and incomplete. It concludes that it is task of the legislator to bring more light in the complicated relationship between private copying and the usage of technological measures.

Three steps forward and two steps back

A second question that the Court of Appeals had to deal with was the possible conflict between the private copying exception and the three step test. The three step test permits to apply an exception in copyright law in certain special cases, namely when the application of that exception does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the rightholder (Article 5 (5) of the European Copyright Directive, Article 9 (2) of the Berne Convention) (cf. EUCD 2001 and Berne Convention). This compatibility of the private copying exception with the three step test is of considerable relevance for the validity of the private copying exception for digital media. In the initial case, the court had argued that distributing copies of DVDs was an act of normal exploitation of films, and that the possibility of making private copies in digital quality would seriously endanger this form of commercial exploitation. In practice, this would mean that the private copying exception would eventually not apply to digital private copies. The Court of Appeals countered this argument and observed, rather reasonably, that preventing a consumer from making a private copy would not imply that the consumer would purchase another DVD with the same content. Moreover, as the Court of Appeals reminded, the interests of rights holders in protecting their commercial interests and investments was already sufficiently safeguarded by the fact that consumers have to pay levies for analogue as well as for digital carrier media exactly for the reason to compensate rights holders for private copies made of a work. Insofar, no conflict between the private copy exception and the three step test could be detected, so said the Court of Appeals.

Copies for parents are private use

In a next step, the Court of Appeals had to look more closely at the question of what a private copy actually is. The opponents argued that Stèphan P., who wished to make a copy for his parents, could not invoke the private copying exception. A copy for one's

parents was not intended for the own, personal use of the person making the copy, so said the court of first instance. Again, the Court of Appeals disagreed. The possibility to make private copies is not restricted to the domestic sphere of the person making and using the copy. It can extend, to a limited extent, also to the family circle. In other words, making a copy for one's parents could be covered by the private copying exception. In this context it is worth mentioning that in most member states a substantial body of national legislation exists on what constitutes private copying, how many copies can still be considered private copying and whether the person copying and using the copy must be identical (for an overview, see Euro-Copyrights.org; cf. sources).

The ability to make private copies is a legitimate expectation

The decision is also ground-breaking insofar as it touches upon aspects of general consumer protection law. The Court of Appeals clarified that the possibility to make copies for private use constitutes an essential characteristic of a DVD. It, thereby, approached one of the crucial and still unsolved questions concerning the relationship of general consumer protection law and copyright law: whether general consumer protection law can be invoked in order to protect legitimate or reasonable expectations that consumers might have on grounds of copyright law, such as the possibility of making copies for private use.

As Schaub (2005) explained, the notion of legitimate or reasonable expectations is key to the application of consumer protection law. Consumer expectations would play a crucial role in determining whether a certain product or a contract relating to it is lawful. So far it was unclear , whether consumers could reasonably expect being able to make private copies of a DVD, applying to the rules provided by general consumer protection law on contracting, unfair commercial practices, defective products and labelling. The question was denied by the court of first instance. As opposed, the Court of Appeals made very clear that the notion of legitimate expectations can also include expectations that flow from copyright law. This is an important step towards improving the legal standing of consumers, as users of copyrighted works. According to the Court of Appeals, expecting to being able to make private copies is not silly at all.

Bottom line

The decision of the Court of Appeals is an important step towards strengthening the position of consumers as regards the use of technical anti-copying measures. It also adds considerably to the ongoing debate about the relationship of technical anti-copying protection measures and the private copying exception. Probably its main conclusion is that the legislator has to clarify this relationship, and that the private copying exception is not at the free disposal of rights holders. This finding may also be interesting for a related question, namely whether the private copying exception can be limited contractually. One example are the user conditions of Apple iTunes, according to which a consumer who purchased a playlist is allowed to copy it at most to seven devices. For the time being, it is still an open question whether iTunes is entitled to impose its particular definition of what private copying is on consumers. Following the decision of the French court, one could argue that the decision of what private copying entails and where its limits are is reserved to legislators and judges, not to private parties. Moreover, the appeal decision prepares the grounds for the application of general consumer protection law in cases where consumers find that the products they have bought prevent them from using this product in a way that is in conformity with copyright law. The court expressed explicitly that consumers can reasonably expect being able to make private copies from a DVD they buy.

Sources

- Berne Convention: http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html
- Court of Appeals, Paris (2005): Cour d' Appel de Paris, 4ème chamber, section B, arrêt du 22 avril 2005, Stéphane P., UFC Que Choisir/Universal Pictures Video France et autres, available at: http://www.legalis.net

- EUCD (2001): Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf
- Euro-Copyrights.org: http://www.euro-copyrights.org
- Helberger, N. (2004): It's not a right silly! The private copying exception in practice. INDICARE Monitor vol. 1, no. 5, 29 October 2004; http://www.indicare.org/tiki-read_article.php?articleId=48
- Schaub, M. (2005): A breakdown of consumer protection law in the light of digital products, INDICARE Monitor vol. 2, no. 5, 29 July 2005, http://www.indicare.org/tiki-read_article.php?articleId=123
- Tribunal Paris (2004): Tribunal de grand instance de Paris 3ème chambre, 2ème section, Stéphane P., UFC Que Choisir/Société Films Alain Sarde et, Jugement du 30 avril 2004, available at: http://www.legalis.net

About the author: Natali Helberger is senior project researcher at the Institute for Information Law, University of Amsterdam. She specialises in the regulation of converging media- and communications markets, electronic control of access to information and the interface between technique, media and intellectual property law. Contact: + 31 20 525 3646, helberger@jur.uva.nl

Status: first posted 25/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=132

Attitudes towards DRM in the Independent music sector

Some insights from interviews

By Philipp Bohn, Berlecon Research, Berlin, Germany

Abstract: Although the major music industry is usually the focus of discussions about digital distribution and DRM, Independent music is a factor whose importance is growing. This article describes attitudes and strategies along the value chain of the Independent music players: labels, content aggregators, technical service providers and distributors. The information provided is mainly drawn from interviews with these actors.

Keywords: economic analysis – business models, DRMS, independent labels, music sector, stakeholders

The growing importance of Independent music

Big online retailers like iTunes or MSN need Independent content to offer a broad range of music. In 2003, the market share of Independent music on the world market was 25.3 % and 19.4 % in Europe (cf. IMPALA). In the United States, Nielsen SoundScan found that content delivered by Independent-owned labels makes up 27.5 % of the retail market volume (Morris 2005). According to the British Association of Independent Music, Independent music averaged 21 % of sales in digital format in the top 75 chart of week 15 / 2005 (cf. AIM 2005). Apple's iTunes Music Store claims to offer tracks by more than 1,000 artists signed with Independent labels (cf. Apple 2005).

To better understand the DRM and online strategies in the Independent music business, we have interviewed various players along the value chain, from labels to download platforms.

While major labels have the market power to pursue their own DRM strategy, Indies often have to accept the license conditions of content distributors – and these requirements are often at odds with those of smaller labels.

Independent labels form a multifaceted group, ranging from very small businesses that primarily market the music of their creative founders, over labels that use the majors' distribution channels for their music, to labels that are co-owned by one of the major media concerns (EMI, Sony BMG, Universal, Warner). These affiliations also influence attitudes towards DRM.

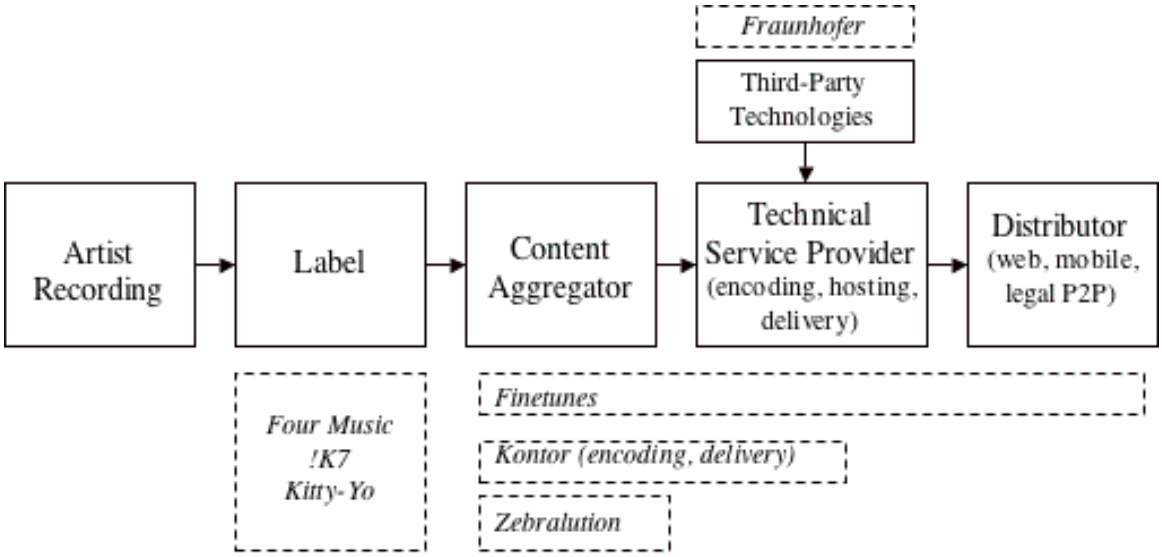


Figure 1: The value chain in the Independent music sector (*Note:* The companies mentioned are those interviewed. The figure is solely meant to position the stakeholders.)

Independent labels

Kitty-Yo (Berlin, 16 artists, 8 employees): If possible, the label licenses mp3 or wav-files DRM-free. But in the end, large-scale distributors, among them iTunes and musicload, decide, concedes *Peter Armster*, then a production manager at the label. It is only the smaller download shops that go with the label's opinion: that once a customer has bought a song, he or she should be free to do with it as pleases – within the bounds of private use, he says. DRM-enabled business models like P2P, subscription and mobile music are being considered, but not yet realized. Creative Commons Audio licenses are not used, as there is no demand on the sides of the artists.

!K7 (Berlin, Hamburg, London, New York City, Tokyo, 30 artists, 10 employees): The label's founder and CEO, *Horst Weidenmüller*, has taken radical steps: he has decided to abandon active DRM and the CD-covers even say so: "Copy Protection Free". The label strongly believes in the possibilities of online distribution. Distributors and labels will have the opportunity to bill one cent for a single music streaming or 20 € for a full album featuring additional content and artwork, Mr. Weidenmüller predicts.

!K7's content is sold DRM-protected via major stores like iTunes, but also via finetunes in unprotected mp3- or ogg-format. DRM supposedly is an issue raised by the major industry and reveals an anti-consumer attitude. The customer relationship should rather be one of "two-way loyalty", he demands.

Four Music (Berlin, London, 20 artists, 8 employees; note: Sony BMG holds a 50% stake): Online business amounts to less than 5% of overall sales of this label. Considerable growth is expected and online business is an important part of the market strategy. The label must abide by the policy of the download shop, but tries to bargain protection as convenient as possible for the consumer. Four's sub-label, London-based Fine Records, for example, uses Beatport (see below) without any DRM protection. If possible, the label employs watermarking, i.e. passive or "forensic" DRM. This would make copyright offenders identifiable while not restricting consumers' private usage, *Markus Roth*, the label's new media director, assures.

Business models that are based on active DRM – such as subscription services – are very attractive for the company, which already supplies Napster's subscription service. Legal P2P platforms such as Peer Impact are also viable distribution channels, although not at the moment. Mobile music is an option once hardware and infrastructure

are advanced and affordable enough, according Mr. Roth.

Content aggregators

Online distributors cannot negotiate with every single label. Content aggregators act as rights intermediaries between Independent labels and download shops, bundling and licensing the libraries on behalf of the participating labels and artists. They often have to act as a buffer between the needs of the labels they represent and the DRM requirements of major download stores.

Zebralution: Independent labels usually lack the personnel and financial resources to deal with major digital stores; and the stores are not interested in contacting every single independent label. Zebralution represents about 100 labels, a catalogue of 20,000 songs and supplies 150 online shops. It delivers content to major online retailers AOL, iTunes, Microsoft MSN, Sony Connect, T-Online and OD2.

According to *Sascha Lazimbat*, Zebralution's head of business, no single artist or label strictly insists on DRM protection. One of the shops the company supplies – 24-7 MusicShop – sells music by major labels DRM-protected, while it sells Independent music unprotected.

Distribution over Peer-to-Peer (P2P) networks is managed using technology developed by Snocap, the company founded by Sean Fanning of Napster fame. When it comes to business models like subscription, the Independents' attitude towards DRM is more favorable. The industry expects growing demand for services like these.

A number of the Indies' songs are popular enough to be marketed as ringtones. Monophonic ringtones are protected by OMA DRM 1.0. Until OMA DRM 2.0 is fully available, main distributors stick to SDC's DRM protection (Swiss company SDC offers a Java-based mobile DRM technology). In the US, bliptones is trying to establish itself as a download platform for ringtones based on Independent artists' music.

Kontor New Media: A competitor to Zebralution, Kontor represents Independent labels dealing with download, mobile, subscription and P2P platforms. With consumer satisfaction in mind, *Michael Pohl*, head of new media, prefers watermarked mp3 files. He explicitly mentions Fraunhofer's Light Weight DRM system (see below). Kontor delivers content to major online retailers AOL, iTunes, Microsoft MSN, Napster, Rhapsody, Sony Connect, and OD2. Both companies also offer consultancy, marketing and coaching services.

The German Association of Independent Labels and Producers (VUT) also fulfils functions of a rights intermediary. For example, it offers members a frame contract if they want to make their libraries accessible to subscription services like Napster. It is interesting to note that VUT has decided not to supply subscription services like Yahoo! Music Unlimited. This is because the service openly acknowledges offering music to sell advertisements for its websites, says *Eva Kiltz*, VUT's general manager. This attitude hints at the self-image of the Independent business: to make money but at the same time uphold artistic credibility.

Third-party technologies

One technology already mentioned earlier is digital watermarking. With the help of a watermark, the person who has bought a certain file can be tracked back in case of infringement. However, the technology does not actively limit the consumer's usage rights.

Light Weight DRM: The Fraunhofer Institute for Digital Media Technology – a German institute for applied research and part of the Fraunhofer Gesellschaft – has realized the needs of Independent music distribution. Light Weight DRM (LWDRM) is a passive DRM system that combines watermarking technology with a personalized digital signature. LWDRM permits copying of content for private use. Due to the personal signature, illegally shared files can be tracked. Thus, the system provides both for the consumer's and the content provider's need for convenience or security respectively. It is employed by download shops such as finetunes (see below). Of course no DRM system – be it active or passive – is completely unbreakable

as *Patrick Aichroth* of the Fraunhofer Institute confirms.

Audible Magic: One of the leading British Independent labels, V2, has just signed an agreement with Audible Magic (Business Wire 2005). Audible's technology allows the tracking of files registered with their database within P2P networks, using digital fingerprints.

Beth Appleton, V2's new media and business development manager, stresses the importance of a good relationship between content providers and consumers to make this business model and security system work: "we trust that they [i.e. the consumers] understand the implications of sharing such files illegally".

Online distributors

In order to distribute music online, there must be download portals selling the library catalogues of labels and artists. They are the digital equivalent to the traditional "brick and mortar" record stores. Some platforms specialize in Indie music and their attitude towards DRM is very much in sync with the content providers – unlike major platforms like iTunes or musicload that usually comply with the majors' DRM strategy.

finetunes: The company offers distribution and encoding services, an own download shop and white-label shop solutions. The shop solutions are licensed to anyone establishing their own online distribution system (labels, Internet service providers, retail brands, music magazines, etc.).

According to *Felix Segebrecht*, head of marketing and shop solutions, finetunes employs a proprietary watermarking system along with Fraunhofer's LWDRM. Active DRM would increase support-expenditures due to interoperability problems between devices and systems.

Mr. Segebrecht distinguishes between two different subscription schemes: renting music (like Napster To Go) or subscription to a fixed number of tracks per month for a bundled price. Superdistribution with peers receiving a cut from profits is regarded to be rather unattractive from the consumers' perspective – they can hardly be expected to enrich themselves by selling music to their friends.

If it spots copyright offenders operating within P2P networks, finetunes usually does not take legal action, which is considered to be too costly. Sales figures are climbing despite online piracy. Fighting infringement is a moral, rather than a legal and technological challenge: an "honest" offer in combination with "gentle pressure" and mutual trust is expected to prove a successful strategy.

Beatport: This online distributor is deeply rooted in the dance-music scene. It caters to fans of this genre, a large proportion being DJs. The music is formatted in high-quality mp3, mp4 or wav, usually featuring 320 kbit/s compression.

Beatport completely abstains from active DRM protection. It would not be acceptable in a tight-knit music community that is based on mutual trust, says the company's director of European sales, *Ronny Krieger*. As about two-thirds of the customers are DJs (amateurs included), files must be compatible with Native Instrument's Traktor DJ-software, which does not support any active DRM system.

Also, the portal is not interested in DRM-based business models. Subscription is not an attractive option for the customers. Prelistening 30-second snippets does not make sense, given the notorious length of dance-music songs.

All files are watermarked. Customers either accept this policy or simply do not care. A song watermarked by Beatport has been spotted on P2P networks only once (P2P networks are not tracked systematically, however). The company issued the offender a caution and refrained from engaging in a lawsuit.

Again, among the labels using the portal for online distribution, there is not a single one insisting on DRM-protection, Mr. Krieger affirms. The company feels that legitimate buyers of digital music should not have less usage rights than those downloading pirated material.

Bottom line

It is interesting to note three major differences for the Indies in comparison to the majors' perceived strategy of active and extensive DRM-protection. First, the smaller and more independent the label, the more sympathetic it is to consumers' convenience and perceived rights. Second, Indies try to avoid active DRM whenever possible. But they acknowledge that this decision is up to the distributor. Third, Independent labels' preferred DRM strategy is a passive one: watermarking. They feel that this does not limit their customers' convenience and at the same time identifies users in case of infringement.

Sources

- 24-7 MusicShop: http://www.247ms.com
- Apple Music Store: http://www.apple.com/itunes/store (last visit 08/19/2005)
- Association of Independent Music (AIM) (2005): http://www.musicindie.org/intro/news/documents/wk15data.doc
- Beatport: https://www.beatport.com/default.php
- Bliptomes: http://bliptones.com
- Borland, John (2005): Indie record labels seeing gold. Online available at: http://news.com.com/2102-1027_3-5805283.html?tag=st.util.print
- Business Wire (2005): V2 signs agreement with Audible Magic Corporation. Online available at: http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20050801005890&newsLang=en
- finetunes: http://www.finetunes-solutions.de/
- Four Music: http://www.fourmusic.com
- IMPALA – Independent Music Companies Association: http://www.impalasite.org/fr02-cont.html ("industry", "Facts and figures")
- Kontor New Media: http://www.kontornewmedia.com/english/news.asp
- Lightweight DRM: http://www.lwdrm.com/eng
- Morris, Chris (2005): Indie label trade group recruiting in L.A. Online available at: http://news.yahoo.com/s/nm/music_indies_dc&printer=1;_ylt=AsoRNWGbRnpx.emlHjIQBB3K.nQA;_ylu=X3oDMTA3MXN1bHE0BHNlYwN0bWE-
- Native Instruments: http://www.nativeinstruments.de/index.php?id=djline_de
- Rosenblatt, Bill (2004): 2004 Year in review: DRM technologies. Online available at: http://drmwatch.com/drmtech/print.php/3453001
- SDC AG: http://www.digicont.com
- Verband unabhängiger Tonträgerunternehmen, Musikverlage und Musikproduzenten, VUT: http://www.vut-online.de/
- Zebralution: http://zebralution.com

About the author: After having graduated from University of Mannheim (Business Administration), *Philipp Bohn* has joined Berlecon Research as Junior Analyst. He is a member of the INIDICARE-team. Contact: pb@berlecon.de

Status: first posted 19/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=130

Mobile DRM convergence

By: Philipp Bohn, Berlecon Research, Berlin, Germany

Abstract: This year, Microsoft has signed three agreements with players in the mobile entertainment market: Philips, Nokia and CoreMedia. This article compares these deals and identifies its beneficiaries.

Keywords: economic analysis – interoperability, mobile DRM, music sector, standards, stakeholders

CoreMedia: first mover or early adopter?

CoreMedia has recently announced to deliver a secure client DRM-implementation for wireless devices. It is promoted to support interoperability between the Open Mobile Alliance's (OMA) and Microsoft's DRM systems. Due to the company's *Multi-DRM* technology, files can be moved from mobile phones to PCs. A plug-in for Windows Media Player allows playback of OMA DRM protected songs on PCs (CoreMedia Press Release 2005).

Other companies have signed similar agreements with Microsoft earlier this year. In February 2005, Microsoft and Nokia announced mutual technological support, as did Microsoft and Philips in May 2005.

OMA and Microsoft DRM

The OMA is an industry forum composed of fee-paying content owners, hardware and software providers, telecom companies, mobile carriers and manufacturers, and technological enablers. CoreMedia, Microsoft, Nokia and Philips all are members of this body. OMA's standard is open in that all stakeholders are invited to join and contribute to technology development, issue statements and test for interoperability on so-called *TestFests*. According to CoreMedia's website, its OMA DRM-based solution is implemented on more than 250 mobile handsets. It is employed by major carriers and mobile music portals such as Vodafone.

Microsoft's DRM 10 system is proprietary and heavily integrated into its multimedia software (Windows Media Player), its upcoming operating system (dubbed *Vista*) and its *PlaysForSure* interoperability program. Devices featuring the PlaysForSure logo are interoperable with download music stores delivering content protected with Microsoft DRM.

DRM 10 rests on patents held by ContentGuard, in which Microsoft holds a minority stake. The DRM-system is pitched as a security and delivery platform both for PCs and portable devices. But to date there is only a limited range of smartphones playing WMA-files: namely the Audiovox SMT 5600, Motorola MPx200 and Samsung i600 / i700 (however, there are almost 60 mobile phones that run Windows Mobile OS).

Both DRM systems use an XML-based Rights Expression Language (REL): XrML in the case of Microsoft and Open Digital Rights Language (ODRL) respectively. The languages are very similar to each other, although ODRL "is focused more specifically on publishing and media applications" (Rosenblatt 2003).

In collaboration with Microsoft

Nokia: After having launched its own mobile music portal solution for mobile carriers, Nokia announced that its handsets will be interoperable with Windows XP based PCs. The technology partners have agreed on long-term, non-exclusive collaboration. Nokia's music-oriented handsets will support Microsoft's DRM 10 and Media Transfer Protocol (MTP). Windows Media Player will playback OMA DRM-protected files as well as MPEG's AAC codec.

Philips: Only three after the deal between Microsoft and Nokia, Philips announced an agreement with the company from Redmond, which is also long-termed and non-exclusive. According to a press release, "Philips plans to support Microsoft Windows Media Audio

and Video and Windows Media Digital Rights Management 10 (DRM) in its Nexperia family of multimedia semiconductors" (cf. sources). It is also "committed to obtaining PlaysForSure verification" for its products. The Nexperia Mobile Cellular System Solutions are especially designed for mobile handsets and also supports mp3 audio format. Philips claims that 150 million Nexperia-based systems are on the market and one-tenth of GSM / GPRS-handsets use a Nexperia solution (cf. sources).

Who benefits?

Consumers: Without doubt, consumers benefit from DRM-interoperability. They want to transfer music purchased with their mobile handset to their PCs and even accept to pay a premium for this service (Dufft et. al. 2005). So far, this is a one-way street, as CoreMedia's technology does not allow transfer from PC to mobile device. To develop the technology for transferability in the other direction is the responsibility of the wireless developers, says Willms Buhse, CoreMedia's head of marketing.

But portable devices' popularity does not rest on their capability of handling DRM-protected music. Players like Apple's iPod are successful because consumers convert audio files into (DRM-free) mp3s – this is one of the results of the INDICARE consumer survey. DRM-interoperability is a step in the right direction, but it leaves some fundamental problems of mobile digital distribution unresolved – consumers may still feel restricted when it comes to their perceived legitimate usage rights.

Microsoft: Part of the software vendor's strategy is to establish the PC as the center of home entertainment, and interoperability helps achieve that goal (cf. sources). The strategic partnerships can also be considered a challenge to Apple's announcement of cooperating with Motorola and the company's dominance in the music download market via iTunes.

OMA: The agreements are an official recognition of Microsoft's market position and DRM-technology (LeClaire 2005). At the same time, they show that OMA DRM may not yet be the uncontested DRM-standard. This can partially be blamed on the licensing structure proposed by MPEG LA that has so far not been accepted by the market, especially not by the wireless vendors (MPEG LA is a private company bundling and licensing the necessary patents for OMA DRM systems). If these quarrels do not come to a quick resolution, the standard's success might be severely threatened.

Wireless vendors: Nokia reaps benefits both as a manufacturer of mobile handsets and as content distributor. Interoperability with stationary devices increases the value of handsets and content. The moves are also in accordance with Philips' *Connected Planet* vision that intents to enable consumers to access content wherever and whenever they wish (cf. sources). As is the case with Nokia, the value of their products rises the more choice they give their users. Being on terms with Microsoft also give vendors additional leverage negotiating fees with MPEG LA (cf. Wichmann 2005).

Apple: The company from Cupertino seems to lose in the short run. Once the repeatedly announced but still withheld collaboration with Motorola yields an actual iTunes-enabled mobile phone, it should provide at least the same degree of interoperability with OMA DRM.

Bottom line

The agreements hold benefits for consumers, device-manufacturers and digital enablers alike. They provide transferability between mobile and stationary devices, which is partially inherent in the respective DRM technologies that both rely on XML-based RELs. But in order to really benefit the consumer, there must also be transferability from PC to mobile device. Although OMA DRM is dominating distribution of mobile content, it is not uncontested. Agreements with Nokia and Philips acknowledge the leadership Microsoft has gained at least in the desktop DRM-environment. It remains to be seen if Microsoft will gain ground in the mobile environment. Wireless vendors, software developers and online distributors seem to have realized the limits of the "walled garden" principle of locking in their customers.

Sources

- ContentGuard: http://www.contentguard.com
- Core Media Press Release (2005): Secure handshake between the two leading DRM worlds. Online available at. http://www.coremedia.com/coremedia.aspx/company/presse/archiv/2005/20050721-drm-microsoft/language=en/id=93252/20050721-drm-microsoft.html
- Dufft, Nicole et. al. (2005): Consumer survey on digital music and DRM (INDICARE). Online available at: http://www.indicare.org/survey
- LeClair, Jennifer (2005): Philips, Microsoft seal software deal. In: E-Commerce Times. Online available at: http://www.ecommercetimes.com/story/43061.html
- Microsoft Press Release (2004): Microsoft Announces Windows Media Connect Technology, Enabling Seamless Media Transfer Between Windows XP-Based PCs and Consumer Electronics Devices
- Philips Connected Planet: http://www.connectedplanet.philips.com/en/1000_Vision.ASP
- Philips Nexperia Semiconductors: http://www.semiconductors.philips.com/markets/communications/nexperia/
- Philips Press Release (2005): Philips and Microsoft to bridge consumer electronics and PC worlds for digital entertainment. Online available at: http://www.semiconductors.philips.com/news/content/file_1159.html
- Rosenblatt, Bill (2003): Rights expression languages: The key to DRM interoperability. In: Seybold Report, Vol. 2, Number 24, p. 3 – 6
- Wichmann, Thorsten (2005): MPEG-LA's portfolio license – A jumpstart for DRM-based markets?. In: INDICARE Monitor. Online Available at: http://www.indicare.org/tiki-read_article.php?articleId=81

About the author: After having graduated from University of Mannheim (Business Administration), *Philipp Bohn* has joined Berlecon Research as Junior Analyst. He is a member of the INIDICARE-team. Contact: pb@berlecon.de

Status: first posted 26/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=135

The ungrateful task of establishing a new technology

Some lessons from the DRM Strategies Conference 2005

Thorsten Wichmann, Berlecon Research, Berlin, Germany

Abstract: The DRM Strategies Conference, which took place on July 27-28 in New York, showed that establishing DRM technology is a rather slow process. Obstacles like unsolved intellectual property issues, changing strategic focus of DRM solution providers and the need to have DRM integrated in the IT infrastructure of consumers and enterprises make for a very slow penetration. In the long run, especially Microsoft may benefit from this situation.

Keywords: conference report – competition, DRM technology markets, enterprise DRMS, intellectual property, interoperability

Introduction

The DRM Strategies Conference organised by *Bill Rosenblatt* and Jupiter is one of the few major industry events on Digital Rights Management. This year the conference took place in New York from July 27-28.

Unlike other DRM conferences, the DRM Strategies Conference is focused on business issues. Political, legal and societal questions like "What rights should consumers and content owners have?", "Are specific features of DRM compatible with copyright law?" or "What should the government do?", which make up a significant part of more general conference programs and which frequently lead to passionate discussions, played only a minor role. They were mostly restricted to a panel on the implications of the US Supreme Court's decision on the P2P file sharing ser-

vice Grokster. With the Electronic Frontier Foundation's *Fred von Lohmann* participating, however, the discussion on panel and floor contributed enough passion for two conference days.

The focus on business issues provided rather interesting information about the state of the market for DRM technology – insights that often get lost in conferences with a broader focus on societal aspects. Especially when compared with the wants and needs of consumers – as presented on the conference based on the INDICARE consumer survey (Dufft et al. 2005) on the conference – these lessons can help to better understand why DRM systems have certain capabilities and lack others or why they develop in certain directions and not in others.

Many open issues – especially about intellectual property

Generally, the presentations and discussions on most panels gave the impression of an industry with many question marks and many open issues. Most issues discussed at the conference were not totally new. Problems of DRM like missing interoperability or intellectual property issues related to DRM technology, for example, are well-known to the industry. It's only that nobody came up with a solution yet.

This was shown very well in a panel on DRM and intellectual property. INDICARE has already reported about the efforts by MPEG LA to combine many different IP claims into a single patent pool license for the OMA DRM (Wichmann 2005). However, so far these efforts have not led to a solution accepted by all parties involved (see also Bohn 2005a).

So it is quite likely, the panellists thought, that the current state of uncertainty for implementers of DRM systems persists. And the risk from this uncertainty may well be quite significant: One panellist estimated the average total cost of a lawsuit in the DRM field to be around 2 million US $. While DRM opponents might welcome such a situation, since it is likely to slow down the spread of DRM systems, it also has a downside: new services for consumers, where some party insists on DRM being used, might not be introduced.

Market-driven standardisation towards Microsoft DRM technology?

In the end there might be a laughing third party, as another panellist pointed out: Microsoft. Many technology companies have already agreements with Microsoft in place, which cover the use of Microsoft's intellectual property. For them it might be easier to simply settle on Microsoft technology for DRM than taking the risk of getting sued when using other technology. So there might be a market-driven standardisation towards Microsoft DRM technology. Microsoft spends significant money on licensing IP from others and is therefore able to offer the users of its technology indemnity against any infringement lawsuits. One panellist even concluded that clearing IP rights and indemnifying technology users might become the future raison d'être of large technology companies.

However, while such a market-driven standardisation might make life easier for smaller technology companies and also for consumers, it is unclear – to say the least – whether they benefit in the long run from such a strong position of a single company. While DRM solutions that build on a common set of technology will tend to be more interoperable – and consumers want that, as the INDICARE survey has shown –, there tends to be more innovation in a system characterised by different technological approaches.

Sobering state of the e-book industry

This dilemma was also illustrated in a panel on e-books, another topic recently covered by INDICARE (Bohn 2005b). The market for electronic books never lived up to early expectations, and nobody on the panel had the hope that this might change any time soon. It is still a rather small market with an annual turnover of 10 million US $ per year, as the International Digital Publishing Forum (cf. sources) estimates.

The coexistence of several different, not interoperable e-book standards was pointed out as one reason for this situation, as this makes e-books rather unattractive. One candidate

for a market-driven standard might haven been Adobe with its omnipresent Adobe Acrobat Reader. However, Adobe decided at the end of last year that enterprise DRM would be a more interesting market and discontinued its Adobe Content Server, a product used by several publishers of protected electronic texts. One panellist saw this as another blow to the market for electronic text documents. It also shows quite well that market-driven standardisation may well fail if the single party able to drive it decides that the pastures are greener elsewhere.

Enterprise DRM figured prominently

Enterprise DRM figured prominently at the conference, which was divided into sessions of general interest, a DRM tutorial, a media section and an enterprise DRM section. One impression from the conference was that several DRM companies place their bets on the increasing use of DRM systems in the enterprise. Many vendors pointed out that the requirements of the Sarbanes Oxley Act (SOX) (cf. sources) could best be met by enterprise DRM solutions. (The act requires companies, among other things, to make sure that only authorised persons have access to sensitive financial company information.)

However, it is clear that for DRM systems being able to protect spreadsheet or text documents throughout their use in companies have to be part of the basic IT infrastructure of a company. If this protection is supposed to cover also partners, it has to be compatible with their infrastructure, too. Again this makes Microsoft and very few other large software companies obvious candidates for providing this infrastructure. Many of the smaller enterprise DRM vendors presenting at the conference are therefore cooperating with Microsoft.

This strong position of Microsoft in the enterprise DRM sector might also have consequences for consumers. As basic DRM functionality is part of future Windows operating systems, also consumers' PCs will be equipped with this functionality. So technology providers for consumer solutions will have another incentive to use the Microsoft DRM functionality as basis for their solutions.

Bottom line

The conference showed very well that theoretical DRM concepts and consumers' wishes about DRM functionality are one thing. The penetration of DRM technology in the market is quite another one. There are many influencing factors: technical requirements like the need to have DRM systems integrated in the basic IT infrastructure, strategic considerations by vendors about which areas of DRM to focus on, or battles about intellectual property. Settling all the involved issues is a tedious task taking a long time.

Putting all these things together leads to the rather sober conclusion that well-functioning interoperable DRM systems as requested by consumers are probably not soon to come.

Sources

- Bohn (2005a): Mobile DRM convergence. INDICARE Monitor Vol. 2, No 6, August 2005, http://www.indicare.org/tiki-read_article.php?articleId=135
- Bohn (2005b): eBooks - The stony road to success and the role of DRM. INDICARE Monitor Vol. 2, No 5, July 2005; http://www.indicare.org/tiki-read_article.php?articleId=127
- DRM Strategies Conference website: http://www.jupiterevents.com/drm/fall05/
- Dufft et al. (2005): Digital Music Usage and DRM – Results from an European Consumer Survey, Berlin, May 2005; http://www.indicare.org/survey
- Sarbanes Oxley Act (SOX): http://www.sec.gov/divisions/corpfin/faqs/soxact2002.htm
- Website of the International Digital Publishing Forum: http://www.idpf.org
- Wichmann (2005): MPEG-LA's portfolio license – A jumpstart for DRM-based markets? INDICARE-Interview with Lawrence Horn; http://www.indicare.org/tiki-read_article.php?articleId=81

About the author: *Thorsten Wichmann* is founder and managing director of Berlecon Research and member of the INDICARE project team. He has been working on a variety of IT and mobile topics during the recent years. Contact: +49 30 2852960, tw@berlecon.de

Status: first posted 26/08/05; licensed under Creative Commons
URL: http://www.indicare.org/tiki-read_article.php?articleId=136

Digital Media Project – Part II: Chances of an open standard

By: Ernő Jeges and Kristóf Kerényi, SEARCH Laboratory, Budapest, Hungary

Abstract: The Digital Media Project, often referred to as DMP, is the fruit of a "bottom-up" initiative that developed in 2003. Its main aim is to develop the fundamentals of standardized and interoperable Digital Rights Management for digital media. Although the project is making publicly available numerous documents on its website (DMP web site 2005), it is not easy to put the pieces together and to assess the project. Therefore INDICARE has dedicated a two part article to DMP. The present second part tries to assess the project in a critical manner finding out the chances of DMP to establish a *de-facto* or even a *de-jure* DRM standard We see a good chance for it, provided the proposed standard would be mandated, for example by the EU for the European market.

Keywords: opinion – consumer rights, digital media, fair use, interoperability, stakeholders, standards

Introduction

In the first part of the article (Jeges 2005) we presented a brief overview of DMP and its approach. The proposed Interoperable DRM Platform (IDP), as the main outcome of DMP's efforts, is a toolkit, i.e. a set of standardised DRM tools based on "primitive functions" derived from existing digital media systems by investigating several selected use cases. In addition DMP has analysed and listed a large number of Traditional Rights and Usages (TRUs) expressing present users' expectations about how digital media should behave and be usable. These TRUs serve DMP as a yardstick and a means against derailing.

In this article we aim to discuss the chances of DMP's Interoperable DRM Platform to become accepted and widely used, taking into account the present state of technologies and markets related to DRM (relying on the publicly available information). Among others we are seeking the answer to the question whether it makes sense to create an open DRM standard without the support of the current big players.

The DRM business

Today the DRM market, focussing on technology providers for the music industry, is extremely polarized: there is Apple with its own FairPlay DRM technology, licensed to no other company than Motorola, and there is Microsoft with its Windows Media DRM technology licensed to everyone else. Even RealNetworks, the former inventor of Helix DRM, has converted their music store to use Microsoft's technology, only Sony is trying to gain ground with its proprietary ATRAC format. On the MP3 player market iPods are estimated to have a 30 percent market share, Sony's devices close to nil (until recently Sony players had not supported unprotected formats, like MP3!), and everyone else uses Microsoft DRM to be compatible with most on-line music services. From the providers' point of view there is no chance to license neither FairPlay nor ATRAC, so one has to go with Microsoft to be compatible.

So for many it may seem as if the DRM game in the music industry was already decided. The founders of DMP, however, think that there is still room left for a new interoperable DRM standard. The project members, we could also say, the supporters of the idea, are mainly educational and research institutes as well as national telecommunications companies – let it be admitted, not really those who drive the market. There are of course also some industrial partners, among them Japanese mammoth CE manufacturers and American technology providers who have not yet committed themselves to any of today's DRM standards. However, today's business leaders – both technology and media companies – are missing. This is not to say that today's leaders will be tomorrow's winners, but if they were interested, they would have joined DMP, to fight for their interests. On the other hand, it is understand-

able that they are not among the supporters, because they have already created their solutions, hoping those to become standards.

So the situation today is quite different from the times when e.g. MP3 became a standard, as there was no – or hardly any – alternative solution. We could think of those times as a market without competition. This was very important for the development of digital media, as the single MP3 standard opened the market for on-line music. But today, what are DMP's chances to become the laughing third, overcoming Microsoft and Apple in the standards game? We think that beating the big players is not a must for DMP to succeed. By understanding DMP's goals and their methodology, it became obvious that IDP is aimed to be an "umbrella standard", with a loose Interoperable DRM Platform, to form a framework with which others *could be*, *will be* and finally and hopefully *must be* compatible.

Benefits of a loose standard

Till now everyone wanted to ride the growing wave of digital, especially on-line digital music (and later video) distribution, so big companies being first steppers could not wait for a standard to be elaborated. The manufacturers and distributors tried or – better to say – were forced to develop a quick solution to an urgent problem, and thus today we have several independent, and due to the circumstances of their birth, non-interoperable systems.

In order to ensure interoperability and longevity of the standard, DMP's approach is loose in prescribing, but still all-embracing: they start from the past, examine the present needs, hoping to eventually create a standard that will fit future needs. By defining primitive functions DMP is primarily starting from *what* can be done with content on digital media, but does not deal in detail with the issue *how* it can be done: only the information necessary to handle the content, the format of content elements (e.g. metadata, rights, licenses, use data) will be specified. Many technological questions, however, important from the implementation viewpoint, are left open in IDP on purpose. Encryption and compression methods to be used, different media formats and other issues are not specified, leaving the opportunity for competition among different role-players on the market, existing today or appearing in the future. And more, IDP aims not only to work with music or video but also with e-books, images and any kind of content that we can not even think of today.

We see that the hardest goal will be to find the proper balance between looseness and strictness. A standard being too generic means that it can easily become meaningless and empty; even if some or all DRM implementations would comply with it, they could still be incompatible in their essential parts, as a multitude of solutions are left open, and can vary. On the other hand, if a standard is too rigorous, it might turn out not to be future-proof meaning that changing demands in the near future could require newer solutions requiring either new standards, or new versions of the existing ones, which would start the tedious standardization process all over again.

Benefits of an open standard

Who could benefit from an open IDP? It is obvious that consumers are benefiting from compatible devices and services, and from lower prices due to higher competition. Content distributors and device vendors will still have to pay for the DRM solutions they use, however, the price of the DRM inherent in their service and product prices would be less due to a free standard and higher competition without monopolies.

Some might say that for content providers the type of DRM used and occasional incompatibility would not matter, because online vendors would always licence the same amount of content from them – regardless of the used technology. We think, however, that content providers and also creators would also benefit from expected larger sales due to the growth of the on-line markets. Moreover, if a free (e.g. GNU General Public License based) DRM solution, based for example on IDP, existed, everybody could become a "creator". This could even lead for example to the appearance of new forms of employment agreements, where the rights to

the created work (content, programs or documents) remain with the employee.

The only losers of an open standard would be current DRM solution providers, holding monopolies on the market today: if they have to be compatible with new standards, they will loose their monopoly; new solution providers will more easily be able to appear, and this could mean a higher probability for a possible new breakthrough in the world of digital media.

Conflicting interests or common goals

The remaining question is what the motivating force will be that are able to push the current solutions, competing with each other on the market, to become compatible with the IDP? DMP is a not-for-profit organization and their standards will also be free. In principle the common interest in interoperable systems will be shared by all players in the DRM game. But is there any interest like this? Is interoperability really desirable for manufacturers and distributors? We have seen that there would be benefits to some players, but the other opinion is that "incompatibility isn't an unfortunate side-effect of deficient DRM systems – it's the *goal* of DRM" (Felten 2004). We also remember the case of Apple and RealNetworks when the latter created interoperability between the two services (Naraine 2004). The sad fact is that interoperability of DRM platforms is not really the interest of the industry.

Thus in our opinion a possible answer could be the enforcement by governments ensuring interoperable standards. It would be especially salutary, if this could be done by the European Union in the first place. Currently all major DRM providers (licensers) are United States-based and therefore the EU is paying money to them with every Cent we spend for on-line digital media. The benefits for the EU, or any government could be in legally enforcing compatibility and interoperability by mandatory compliance to the standard for every product or service offered on the common market, thus not only serving the needs of the European consumers but also re-opening the market for European players, like newcomers to the DRM technology market, eventually making it to the global market.

We see that the market is moving towards proprietary systems, so in the current situation only governments could enforce interoperability by not allowing non-compatible products (e.g. players) or services (e.g. downloadable music or video) to appear on their markets. We imagine this as the CE sign to be found on all electrical equipment sold in Europe.

If the Interoperable DRM Platform was this mandatory standard, it would have multiple benefits.

- No company could charge for the standard itself, so it would be entirely free to step on the market with any new player or service. This would increase competitiveness and be a "sledge-hammer" to break the rules of current oligarchs (currently Apple and Microsoft).
- An interoperable DRM standard would also directly serve the interests of consumers, since they would not have to worry any more about compatibility issues. It is so good to know that an AA battery we buy in the store will fit in every device, and it would be similarly easy if we could be certain that the purchased songs will play in every player today, and will probably do the same in future products.

Bottom line

Either IDP or any new standard dealing with digital media could presumably not become a de-facto standard without a common interest of DRM solution providers. As this common interest does not seam to exist, it is not surprising, that the current big players are not on the list of the members of the Digital Media Project. We see the chances of success of DMP's standardisation efforts depending on governmental enforcement, for example on the European internal market. This would be essential for both the market of digital media as a whole, including online music and video markets, and consumers, as interoperability is becoming their elementary need, which can only be ensured by a good standard.

Sources

- The Digital Media Project web site (2005):http://www.dmpf.org
- Jeges (2005): Digital Media Project – Part I. Towards an interoperable DRM platform. INDICARE Monitor, Vol. 2, No 4, June 2005; http://www.indicare.org/tiki-read_article.php?articleId=116
- Interoperable DRM Platform (IDP) Functions and requirements, 28/01/2005 http://www.dmpf.org/open/dmp0328.doc
- Interoperable DRM Platform (Technical Specification, Approved Document No. 3), 15/04/2005 http://www.dmpf.org/open/dmp0403.doc
- Cole, Jack (2004): Raising the Bar. IEEE Computer magazine, September 2004 issue
- Naraine, Ryan (2004): Apple: RealNetworks hacked iPod, internetnews.com, 29/07/2004, http://www.internetnews.com/bus-news/article.php/3387871
- Felten, Edward W (2004): A perfectly compatible form of incompatibility, Freedom to Tinker, 15/04/2004, http://www.freedom-to-tinker.com/index.php?p=578

About the authors

The authors are researchers at Budapest University of Technology and Economics in the SEARCH Laboratory.

Ernő Jeges's research areas are mainly focused on biometric security solutions, but he was involved in a number of research activities dealing with IT security and the technology aspects of digital rights. He received an MSc in computer science from BUTE in 1995. Contact: jeges@mit.bme.hu.

Kristóf Kerényi's interests include mobile and wireless IT security, as well as technological aspects of DRM. He received an MSc in computer science from BUTE. Contact: kerenyi@mit.bme.hu

Status: first posted 26/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=134

Managing copyright in a digital world

An introduction to the contributions model and the Rights Office System

By: Nicholas Bentley, Rémuzat, France

Abstract: Is copyright still on the right track? Are DRM systems and Creative Commons licences the only solutions that can support copyright in the digital world? This paper suggests that copyright is founded on a *contributions model* for creating intellectual works and that an exchange of rights to intellectual works would be more productive than continued trade in copies. A *Rights Office* system is proposed as an alternative infrastructure to support copyright and its potential benefits (registered rights, privacy, new business models, non-specialised hardware) for all users, from creators, to commercial users, to consumers, are discussed. The ideas expressed here have been developed with feedback from a number of individuals via Web sites and discussion lists.

Keywords: technical analysis – business models, copyright law, Creative Commons, DRMS, levies

Introduction

This article presents a summary of the *Intellectual Contributions* (Bentley 2005) philosophy and the *Rights Office* system (Bentley et al. 2005) and explains how these ideas might provide an alternative model for regulating intellectual works in the information society. Under the Rights Office system the right of access to intellectual works is considered paramount and the

regulation of copies takes a secondary role. This simple conceptual step makes restricting the distribution of copies by technical measures unnecessary, allows legal copies to compete with illegal manifestations, and introduces a host of social benefits in the spirit of a balanced copyright regime. Analogue copyright is reviewed in the light of a *contributions model* and some of the shortcomings of prominent digital implementations of copyright (DRM, Creative Commons, levy systems) are highlighted.

Intellectual contributions

Many people tend to view copyright as a single stream process: authors produce works that are then edited, processed, and distributed to consumers who take in the content and that is the end of it. More careful analysis suggests that this one-way stream of information is not the correct view and that the "contributions" that go towards a new work come from many sources. Authors and creators rely on many preceding works to feed their creativity either directly or indirectly. If we take a broader view of contributions, where contributions mean any support for the artist (payments, reviews, criticism, recognition, quotations, citations, and recommendations), the contributions model can be still more complex. In the broad context of the contributions model there are many users: some contribute directly to the intellectual content (creators of pre-existing works, the author[s], and the editor[s]), others contribute by way of the remuneration chain (distributors, reviewers and consumers). Figure 1 illustrates some of these activities.

Copyright in the analogue world grants the right of access to intellectual content to the consumer via the proxy of the physical copy (for instance, owning the book). Copyright gives the author the right to receive the contributions from potential users of the work via the proxy of granting her the sole right to print and distribute copies. However, limitations are put on the rights of the original author (first sale, term limits, fair use) to protect the contribution chain, allowing future authors to quote, cite, etc, and allowing consumers to pass-on the physical copy thus disbursing their investment.

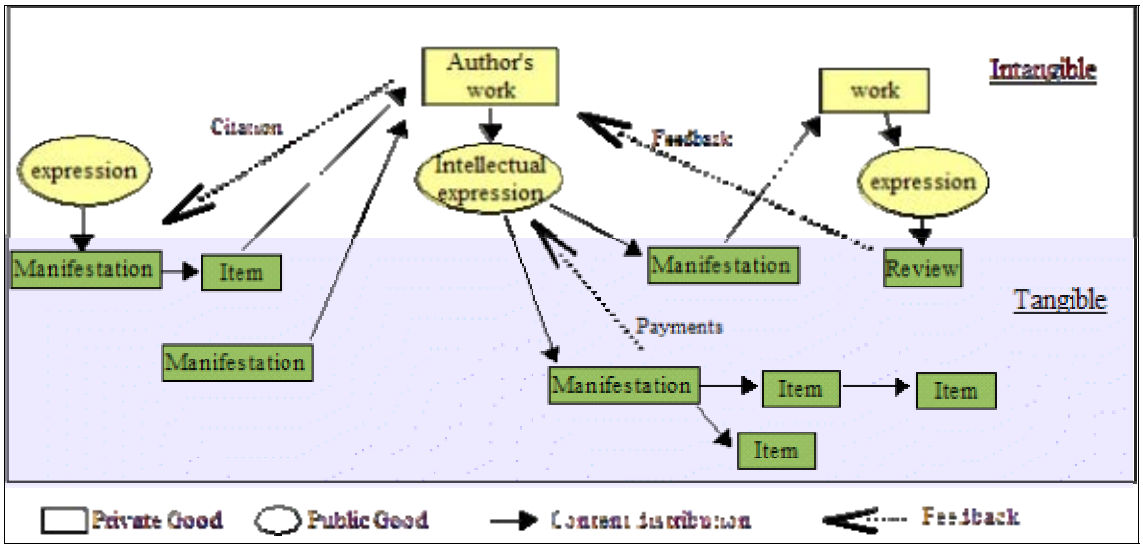


Figure 1: Intellectual contributions in the analogue world

Analogue copyright transforms each manifestation of the work into a *private good* (cf. Wikipedia) and thus provides the tangible structure to support the financial aspects of the contributions model. The limited supply of physical books can be traded to funnel funds to the rightsholder and the author can be identified via these tangible manifestations. Figure 2 shows the liaison between the public/private good and the tangible/intangible elements.

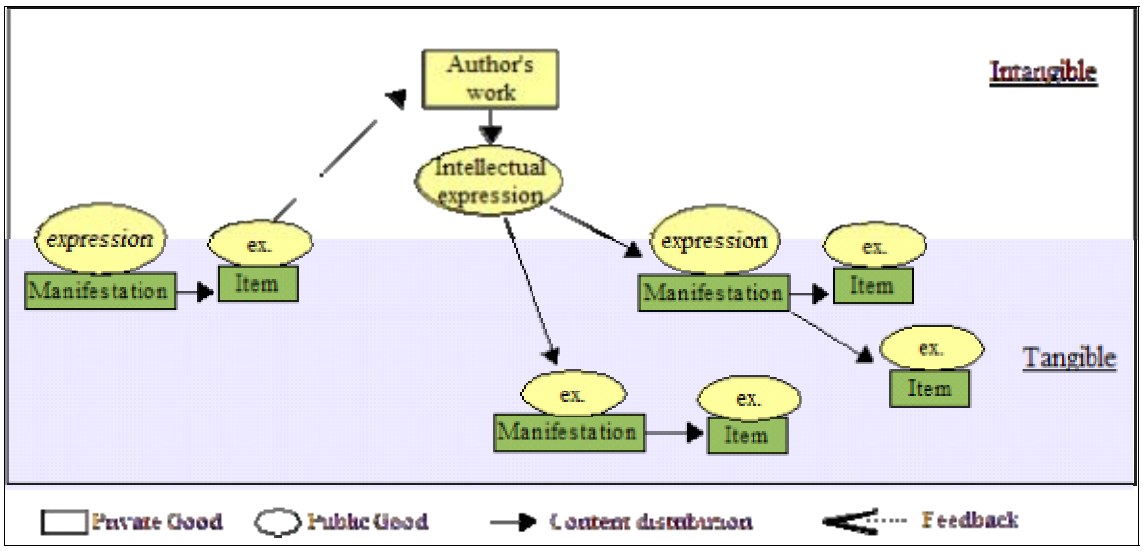


Figure 2: Public/private goods, intangible expressions, and tangible manifestations

Moving to a digital world causes these manifestations to become intangible and the financial part of the contributions chain breaks down when multiple copies can easily travel far and wide. These digital manifestations loose their excludable and rivalrous status and effectively become *public goods* (cf. Wikipedia). Most attempts to maintain a viable contributions model in digital form either try to make the digital manifestations a *private good* again by locking up the content (e.g. DRM) or abandon any idea of restoring the *private good* status and hope for remuneration via another route (e.g. Creative Commons).

Rights Office system

The Rights Office system recognises that in the Intellectual Contributions model the finite creative efforts of the author are the important *private good* and that the author's right to allow contributing consumers to share access to this rivalrous and excludable "effort" forms the fundamental aspect of any economic model. In the digital world the product of this collaborative effort produces a manifestation of the intellectual work that is a *public good* and the Rights Office system does not attempt to make these manifestations rivalrous or excludable. It does, however, insist that the contribution to the creative effort, whether intellectual or remuneration, is recognised in the form of two, unique, persistent, identifiers that record every transaction in the contributions chain. This recognition can be represented (see Figure 3) by a tangible layer in the contributions model that firmly establishes the rights of all users as a regulated resource.

In the Rights Office system, all rights to an intellectual work are recorded in a permanent, secure, location on the Internet. The Rights Office System allocates a dual identifier to each work and further identifiers to any subsequent physical manifestations (copies) of the work. These identifiers are in the form of unique, permanent, Universal Resource Identifiers (URI). The Handle system (cf. CNRI) might provide the persistent infrastructure for these dual identifiers but unlike the Digital Object Identifier system (cf. DOI) that uses one Handle name to identify a work, the Rights Office system uses the names to identify the rights of the users and only subsequently the work or the manifestation involved.

Throughout this paper, by way of an example, we will describe how an author and a consumer will record rights to an exchange of an intellectual work (see Figure 4) although the same principles apply to any users exchanging works in the system (e.g. publisher with distributor, distributor with consumer, etc.). A typical chain might be a publisher transferring distribution rights to a commercial service that then registers access rights to individual consumers.

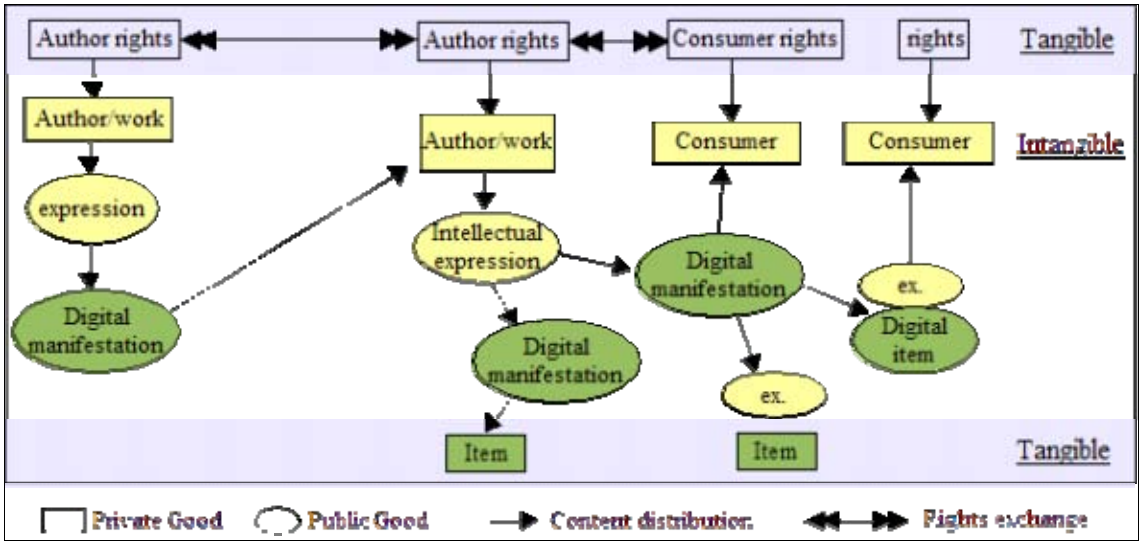


Figure 3: Rights and intellectual contributions

As a right-of-access passes from author to consumer, the system goes through the following steps:

- Two rights identifiers are created; one for the author, recorded in the Authors Rights Office database (ARO), and one for the consumer, recorded in the Consumers Rights Office database (CRO).
- The ARO and the CRO exchange and record each other's identifiers, thus linking the transfer of access rights to the work. The combination of these two identifiers is known as the Product Rights Descriptor (PRD). Thereafter, any copy of this manifestation will, as it goes through life, contain the unique PRD it was assigned.

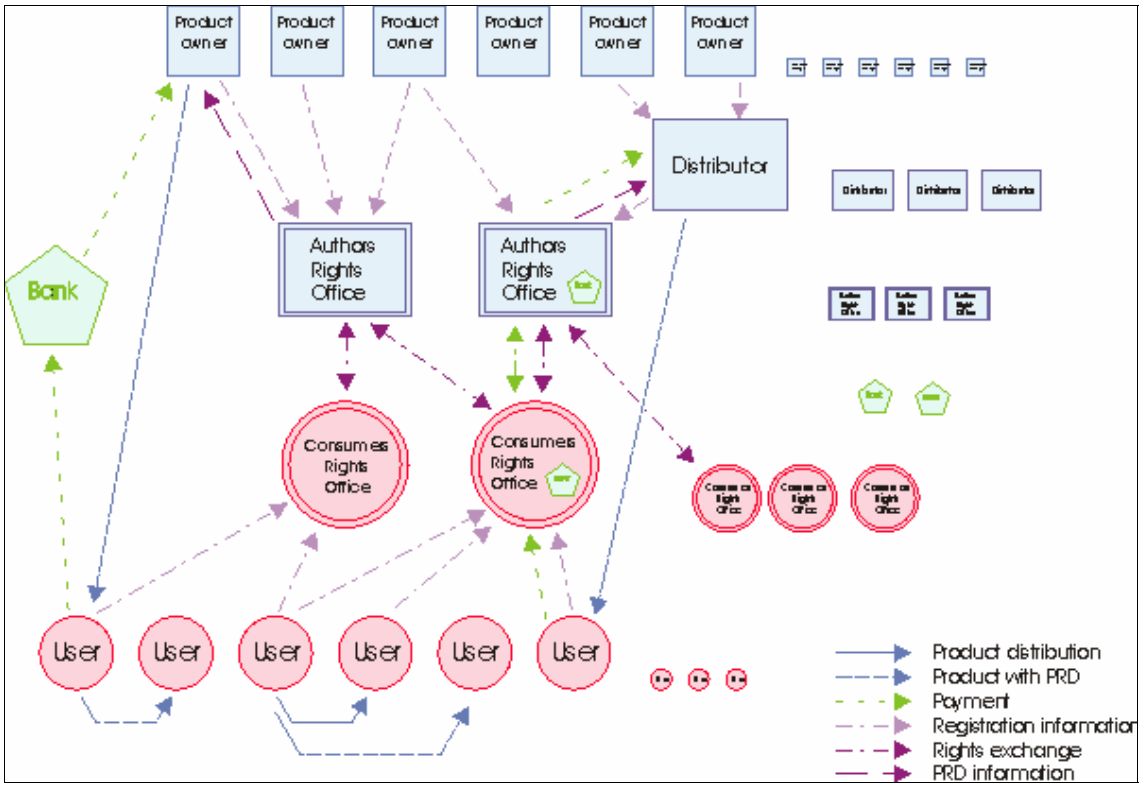


Figure 4: Rights Offices

In the Rights Office environment the independent duel office structure provides the one-to-one exchange that builds trust. Privacy is maintained because personal information is only held in the office that acts as an agent for a particular user and the identifiers attached to the product are effectively anonymous. Identified rights add value, especially for consumers, and more value can be introduced with business models that allow consumer participation in the success of the product. Potentially, these multiple, distributed, "offices" on the web not only provide the backbone for the allocation of user rights but could also provide the "trusted" infrastructure for funds transfer and so might provide the framework necessary for widespread micro-payment transactions. The rights office environment therefore corresponds to the statement of *Simon Nicholson* that "*... the combination of value, trust, and privacy will determine future digital services*" (quoted in Guth et al. 2005)

Why will the Rights Office system work?

The first questions to arise are; "How does the Rights Office system work if there is no mechanical protection of copies?", "Surely unremunerated copies will spread everywhere?", and "What is the incentive for consumers to pay for content?" The short answer is that some copies will become widely distributed but we don't care and the system does not try to track or directly control copies. Some examples on business methods and incentives:

All copies regulated in the Rights Office system will be properly identified and so there is always the chance that a consumer coming across one of these copies will reward the rightsholder. The "chance" that the rightsholder will be rewarded becomes a significant possibility when the rights of the consumer are considered. For instance, the Indicare consumer survey found that "*Consumers are willing to pay for more usage rights and device interoperability*" (cf. Dufft et al. 2005). The Rights Office environment supports these rights, device transparency, and permanent access to the work. The reason why the identification will remain intact is that identified works compete on an equal footing, if not better, with any illegal unidentified copies; there is no penalty for holding a properly identified copy so why risk holding an illegal copy?.

- Copies can be given to family and friends but only one tier of copying is allowed. Someone who is given a copy in this way has no rights to make further copies.
- Sometimes, for the purposes of promotion say, it is a positive advantage that copies are widespread and the fact that these copies will provide a direct link to the rightsholder is a major advantage. "*For independent publishers, wide exposure of their content is a prime promotional tool"* (cf. Bohn 2005)
- The registered partnership between the rightsholder and the consumer allows for business models that reinforce the advantage of having bought rights to the content. e.g. discounts on future products, upgrades, even a model where the consumer could be encouraged to recommend the content to others and receive a partial refund if the third party purchases their own copy.
- Presale of rights to a work could be an option to cover production costs for the artist or author for example. As soon as the work is complete all registered rights holders would have instant access to the work.
- Damaging, unauthorised, third party, commercial use of a work in the Rights Office environment will be naturally limited for two reasons. Either, this unauthorised user will be issuing new identifiers and will risk having his or her illegal act traced to them, or, they will be passing on works to another consumer who won't be given their own identifier. This second act will be unattractive because the receiving consumer could either have probably obtained a "free" copy elsewhere or could have bought a legal copy with all the rights that come with it.

Contributions vs. other regimes

All the articles from the July issue of the INDICARE Monitor (cf. INDICARE Monitor) consider DRM to be the main contender for regulating commercial uses of copyrighted material in a digital world. Creative Commons is usually relegated to the non-commercial sidelines with the odd exception of the likes of Magnatune (cf. Buckman). Here we examine some of the limitations of the various solutions and at the same time compare them to the contributions model.

Contributions vs. DRM

When someone buys an analogue book they create a new intellectual contributions chain. There is only ever one excludable book in this chain (the first one) and this helps define the monetary value to be placed on this chain. If a digital copy of this book is introduced into a new chain the work can be reproduced indefinitely, easily distributed along the new chain (even in a branching fashion) and these public good characteristics make the value of this contribution chain uncertain. DRM, i.e. technology that controls who and how users can use content, attempts to restore a known value to this chain by limiting copies (making them excludable again). The ideal might be said to be a limit of one copy as in the analogue world.

There are potential disadvantages to this DRM modelling of the analogue world from the intellectual contributions point of view:

- The limit of one copy without regard to "fair use" could disrupt the citation feedback chain;
- The "first sale" doctrine, which created a contributing chain, allowing a buyer to recoup some of his contribution while furthering the distribution of the work, could be disrupted; and
- Most significant, chasing the analogue model of copyright destroys the potential advantages of digital distribution. i.e. speed of transmission, access to a wider community, lower reproduction and distribution costs.

The Rights Office system removes the need for any control of content at the hardware level or in the realm of the individual user and hence could remove the considerable technical burden of controlling content from source to destination. The burden of control and regulation is shifted to the "Office" level, where protocols will have to be established and the exchange of rights identifiers fully protected, however this will be orders of magnitude simpler than the full scale DRM approach. Also, all the complexity is one step removed from the average consumer.

Two recent Indicare articles (cf. Knopf 2005, Tyrväinen 2005) argue the benefits to DRM systems if they were to support Fair Use and other copyright exceptions and they offer technical solutions for achieving this. The benefits include trust and consumer acceptance. The Rights Office system, in contrast, considers these exceptions as vitally important and even goes so far as to licence the user to make unlimited copies (provided the identification rules are met). The rational of the Rights Office system is that consumer "rights" are so fundamental to the operation of the contributions model that they should be transferable to the consumer and that once you have taken this step and instituted a system to regulate these rights any form of DRM becomes redundant and could even have a negative impact on the operation of the system.

Contributions vs. Creative Commons

Creative Commons and Rights Office both support the freedom of the rightsholder to choose how they distribute their work and what rights they choose to withhold. Like Creative Commons the Rights Office system is founded on copyright and will rely on a series of licences to specify how the work can be used by third parties. The Rights Office also supports the notion that if someone has a work made available to them they are allowed to absorb the content, thus supporting the "unregulated use" where anyone can read the book (cf. Lessig 2002).

Rights Office differs from Creative Commons as follows:

- The Rights Office licences are granted to individuals and not issued as open licenses. This is of fundamental importance as it establishes the one-to-one relationship between the rightsholder and the user that is essential for the

contributions model and at the same time forms the basis of any commercial transaction.

- Some of the Rights Office licences allow the user to pass on "rights" to third parties. This again is of significant importance because it can establish the user as both a contributor and recipient in the contributions chain and this inclusiveness will lead to more support for the original rightsholder.

To give an example of just one of the licenses in the Rights Office environment, the general licence granted to the average purchasing consumer might start something like this in common deed terms:

> *The consumer who holds a valid identifier to this product is allowed to make unlimited copies to protect their access to the work provided that the product and its identifiers remain intact and unmodified.*

Note how this might lead to the consumer making a copy available to a third party, a friend say, however this third party has no rights to do anything with the product, not copy it, pass it on, nothing accept her basic unregulated use of absorbing the content.

The Rights Office system also offers the exciting possibility of porting some of the Creative Commons licences into the Rights Office environment where they would be able to compete on an equal footing with more restrictive licenses.

Contributions vs. levies

Levies or flat taxes on hardware or services have been proposed and enacted in some cases in an attempt to reward artists for private copying and other uses of the copyrighted work (cf. Tan 2004). One disadvantage of levies is that they are indiscriminate and therefore penalise non-copyright related uses of the service or hardware. Widespread use of the Rights Office system could remove the need for levies because of the possibility of directly rewarding the rightsholder. A second objection to levies is the lack of a means to fairly track usage and funnel funds to the artist in proportion to the use of their work. If it were decided that some levies were still required in the future the persistent identifications generated by the Rights Office system could provide the means to track usage.

Rights Office development status

If the will was there to establish a Rights Office system there is no obvious legal or technical impediment to doing so. The fact that no central control of the numerous distributed Rights Offices is required just as there is no central control of the Web makes the possibility of establishing a global system more feasible. Users who decide to use Rights Office could have their products compete with other intellectual property distribution methods and the best would win out. Some of the practical obstacles and steps to be taken can be listed as follows:

- Promotion of the subtle principles involved in exchanging rights in the Rights Office system, such as, how the independent Rights Offices will tend to be self regulating, and how legal copies can compete with illegal copies.
- Development of open Rights Office protocols.
- Development of an initial set of standard licenses.
- Development/adoption of the appropriate persistent identifier framework.
- Implementation of a basic Office system and user interface.
- Enforcement of the principle that a work should not be separated from its identifiers would need to be vigorously supported with a publicity campaign and where necessary legal sanctions.

Bottom line

The Rights Office proposal offers a formal system for regulating copyrighted works in a digital environment that removes the need to restrict digital copies by DRM or any other technological solution. Distributed "Rights Offices" provide a self-regulating, end-to-end, rights trading environment that can support many business models from free promotional distribution to restricted, single customer, streaming models while maintaining privacy and allowing for copyright limitations. Maybe the "*bottom line"* in the digital files of the future should

contain the Product Rights Descriptor, the identifiers that establish the rights of access of all users, along side the copyright © –

Document Product Rights Descriptor:
http://www.commonrights.com/RightsOffice/ARO-126.htm#ARO1
http://www.commonrights.com/RightsOffice/CRO-500-CRO1.htm

Sources

- Bentley, Nicholas (2005): Intellectual Contributions; http://www.omidyar.net/group/intellectual-contributions/ws/ic_rights
- Bentley, Nicholas et al (2005).: Rights office and distributed intellectual property rights (DIPR) system; http://www.commonrights.com
- Bohn, Philipp (2005): eBooks - The stony road to success and the role of DRM. INDIARE Monitor Vol. 2, No 5, July 2005; http://www.indicare.org/tiki-read_article.php?articleId=127
- Buckman, John: Magnatune Embraces Podcasting. Interview by Podcasting News; http://www.podcastingnews.com/articles/Magnatune_Embraces_Podcas.htm
- CNRI (Corporation for National Research Initiatives): Handle System; http://www.handle.net/
- Creative Commons: http://creativecommons.org/
- DOI (Digital Object Identifier System): http://www.doi.org/
- Dufft et al. (2005): Digital Music Usage and DRM – Results from an European Consumer Survey, Berlin, May 2005; http://www.indicare.org/survey (section 4.2)
- Guth, Susanne; Iannella, Renato, Serrão, Carlos (2005): ODRL workshop 2005 report. INDICARE Monitor, Vol. 2, No 5, July 2005; http://www.indicare.org/tiki-read_article.php?articleId=126
- INDICARE Monitor, Vol. 2, No 5, July 2005; http://www.indicare.org/tiki-page.php?pageName=IndicareMonitor#TOCV2N5
- Knopf, Dominik (2005): How to implement copyright exceptions in DRM systems. INDICARE Monitor, Vol. 2, No 1, March 2005; http://www.indicare.org/tiki-read_article.php?articleId=87
- Lessig, Lawrence: Free Culture. Keynote from OSCON 2002; http://www.oreillynet.com/pub/a/policy/2002/08/15/lessig.html
- Tan, Sze: Levies: A Possible Panacea. Posted to Mailing list of “Law in the Internet Society,” Columbia Law School on 21 Nov 2004; http://emoglen.law.columbia.edu/LIS/discuss/118.html
- Tyrväinen, Pasi (2005): Fair use licensing in library context. INDICARE Monitor, Vol. 2, No 2, April 2005; http://www.indicare.org/tiki-read_article.php?articleId=94
- Wikipedia: Private good; http://en.wikipedia.org/wiki/Private_good
- Wikipedia: Public good; http://en.wikipedia.org/wiki/Public_good

About the author: *Nicholas Bentley* is an independent designer with a background in information technology who has passionately followed the digital intellectual property debate over many years. Contact: Nicholas@commonrights.com

Status: first posted 26/08/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=133

Editorial of INDICARE Monitor Vol. 2, No 7, 30 September 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: One focus of the present issue of the INDICARE Monitor is *online music*: on the one hand we report about the trend-setting music fair Popkomm, on the other hand we descend to China's and Hungary's online music realities. The second focus is on *B2B relations*: between online music providers and collecting societies, between publishers and libraries, and between the actors in the educational publishing market. Finally, we present the findings of a Technology Assessment on digital rights and DRM carried out in Denmark.

Keywords: editorial – INDICARE

About this issue

Online music here and elsewhere

The issue starts with a country report about China written by *Anna-Lucille Montgomery*, a researcher from Australia. Her article is based on desk research and interviews with Chinese experts. The subject is the online music market in China, which is embedded in the broader picture of ICT penetration, social habits and legal developments since China became member of the World Trade Organisation. It is against this background that the potential role of DRM systems and innovative business models is discussed. She concludes that "consumers who are used to receiving content for free will not willingly shift to a system which expects them to pay" and "the copyright environment in China may force intellectual property owners to move away from a royalty-based system for content provision".

The next article moves us from Far East to Eastern Europe, but the topic of online music is still the same. *Kristóf Kerényi* shares his hands-on-experience with online music services in Hungary. He describes his experiences as distressful: limited choice, high prices and low level of service. No wonder that in this situation file-sharing as well as illegal music and video downloading are dominant. Consequently "DRM-based services will have to become a lot better to beat the free offerings of the (dark)net". However, without competition, this won't happen.

Nicole Dufft attended Popkomm 2005 in Berlin, one of the important music industry fairs, a place to watch out for new developments in the online music business. She found that the hype about DRM has decreased. From being a prominent topic onstage it apparently turned into a mere technical problem, and this type of problem is usually dealt with backstage. The hot topics of the fair were: mobile music, podcasting, new radio formats, and subscription services vs. a-la-carte downloads. Nicole regards the music industry as "becoming more creative and innovative" offering better services to consumers.

B2B business models with or without DRM

The next issue is again about online music, and it is about B2B DRM. *Margreet Groenenboom* is carefully explaining the "Study on a community initiative on the cross border collective management of copyright" prepared by the European Commission and released 7 July 2005. It is worth mentioning that the paper is based on a stakeholder consultation and that presently the consultation of stakeholders goes on (80 reactions so far).

In this paper the Commission reflects how cross border licensing practices might be improved. The most important stakeholders are on the one hand online music shops striving to deliver their services throughout Europe, and collecting societies with whom licenses have to be negotiated. The current situation requires rethinking the role of collecting societies, and an assessment of the potential of DRM systems to make this licensing business more effective. I imagine a good solution would help to solve some of the problems *Kristóf Kerényi* described for Hungary. In my view it is important here, not to mix up B2B DRM with B2C DRM. Effective solutions of this cross border licensing issue will probably rely on B2B DRM, but

this assumption does not say anything about the need of B2C DRM.

The licensing relationship between academic publishers and libraries is the topic of the next article dealt with by *Brian Green*, an outstanding standards expert in the publishing business. The question is how digital rights should be managed in the B2B relation between academic publishers and libraries. This is an issue, because the number of digital resources in libraries is growing and libraries have to cope therefore with many different licensing terms. What is needed are appropriate metadata standards. Brian Green reports about initiatives and the state of the art in this field. In his outlook he states that"... in addition to the technical work remaining, there are still several practical and political issues to be dealt with". Among them is the concernthat the development of these metadata standards may lead to the introduction of DRM enforcement technology into the relationship among publishers, libraries and library users. Brian Green is convinced that this worry is unfounded.

Paola Mazzucchi, AIE (Associazione Italiana Editor), presents findings of the OrmeE project funded by the European Commission's eLearning programme. OrmeE stands for the "Observatory on Rights Management for eLearning in Europe". Its perspective is the role of educational publishers in the emerging transnational e-content market.

Traditional textbook publishers have to deal with new competitors, among them companies specialised in e-Learning or technology companies. In this new market, content providers, aggregators, and distributing intermediaries have to find business models (9 types of constellations are presented in the article), which meet the needs of the educational world. Licensing models to be adopted are a crucial issue, and in this context DRM has become a topic of discussion. Among the current problems of educational publishers highlighted by Paola Mazzucchi is the poor adoption of complex DRM systems by educational publishing houses, and the lack of a truly harmonised legal framework. In her words:"... despite the stated goal of harmonising national copyright legislations, the implementation of the 2001 Directive has not yet achieved much in making the exceptions in the field of educational uses converge. It is therefore crucial to find and support best practices that demonstrate the actual possibility to combine copyright protection and effective access to content by educational organisations and individual learners".

Technology assessment of DRM in Denmark

The final article of this issue, titled "Digital rights in the information society" presents the result of a study about "consequences and implications of digitalisation and DRM" carried out by the Danish Board of Technology. A working group of stakeholders was set up to debate and outline a new balance between consumers' and rightholders' interests. However, insufficient practical experience with DRM systems and a divergent understanding of what DRM really is, turned out to be a major obstacle to achieve this goal. Nevertheless the concerns and recommendations, as described by *Jacob Skjødt Nielsen* are very interesting. Just to highlight some of them: one recommendation is to intensify cooperation between ministries in these matters, another to organize further consensus building activities with a long-term perspective in mind. A need for new usage rights, a need for interoperability and open standards, and a need to gain more experience with DRM in the public sector were further points. All in all, the debate in Denmark appears to be rather similar to the debate in other comparable European countries – in other words: the Danish Technology Assessment is a piece of European debate.

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 30/09/05; licensed under Creative Commons
URL: http://www.indicare.org/tiki-read_article.php?articleId=145

Online music markets in China

The broader picture and the role of copyright and DRM

By: Lucy Montgomery, QUT, Brisbane, Australia

Abstract: China is one of the most difficult markets in the world for copyright owners. Illegal distribution networks are well established and consumers are used to content that is either free or very cheap. China's legal system is still in the process of developing and the Chinese government regularly fails to enforce its own IP legislation. As a result, translating formal rights into royalty payments is extremely tough. This article, which is based in part on interviews by the author, describes the present communication infrastructure, social habits, and the copyright environment in mainland China. Against this background the potential role of DRM systems and innovative business models is discussed.

Keywords: country report – business models, consumer expectations, copyright law, music markets, piracy – China

Music downloading and sharing in China

At present, rates of music piracy are high throughout China's audio-visual industries. Music industry executives generally quote piracy rates of between 75% and 95%. Disc piracy is common, particularly in wealthier cities along China's eastern seaboard. People living in less affluent or developed areas still use pirated audio cassettes, which are cheaper to copy than digital media. Cassette players, which are capable of both playing and copying music, are much more affordable to people living in poor areas of China than computers. They are also easier for less educated sectors of the population to use: they do not require computer literacy or the ability to Romanise Chinese characters (pin yin). Expensive hardware investments are also unnecessary, allowing anyone with a tape recorder and a blank cassette to copy and share music using this format, regardless of their access to the internet.

At the same time, the development of an extensive broadband network in China's cities and growing levels of PC ownership among the emerging urban elite are also resulting in high levels of music downloading. MP3 downloading is particularly common among university students and young professionals, who are more likely than other sectors of China's population to have access to the Internet, an interest in music and the skills to engage in this activity.

Consumers have no incentive to pay for MP3 downloads. Chinese Internet search engines such as baidu (http://www.baidu.com.cn) and emule (http://www.emule.com.cn) provide fast, free, easy music downloading. To date, members of the public have never been prosecuted for downloading music illegally, although action has been taken against some websites by copyright owners (China Economic Review 2005).

Music labels such as Sony have been involved in high profile events aimed at raising awareness of the impact of piracy on the music industry and on artists: in November 2003 between 50,000 and 60,000 people packed Shanghai Stadium for the Asia Superstar Anti-Piracy Rally Concert.

China's central government has undertaken a number of publicity campaigns encouraging consumers not to purchase pirated audio-visual products, including television and billboard advertisements with slogans such as "be a good Beijinger, resist piracy". In spite of these efforts, Chinese consumers face little, if any, moral stigma related to music downloading. Consumers are now used to downloading music without paying, and even if they did want to download legally, few legitimate services are available. According to *Beaker Huang*, Marketing and Business Development Director for Warner Music, China, it took Warner a long time to realise that university students were not their biggest market, but their biggest liability:

"…as soon as they get to college the only way they are going to be spending money on music is they keep on spending money to upgrade their PCs so that they can be downloading more songs." (Montgomery 2005a).

PC ownership and access to the Internet

Internet access is growing rapidly and MP3 players are cheap and readily available. According to CNNIC (2005) there are 103 million internet users in China, 53 million of whom have broadband. High speed broadband networks are being rolled out in most urban centres and China is expected to have 34 million broadband subscribers by the end of 2005. This is impressive, when compared with the United States – which has 39 million subscribers. By the end of 2007 China is expected to have 57 million broadband subscribers, compared with a projected 54 million in the US (Reardon 2005). Although at present only about 2% of Chinese households own PCs (Kessler 2004), this number is growing fast. By 2010 it is expected that 178 million new PCs will have been purchased in China (BBC 2004). Internet cafes are still playing an important role in providing access to the Internet. This has significant implications for the types of online music models that new media developers might choose to apply in China. According to *Ruuben van den Heuvel*, Vice President of digital business Asia at Sony BMG: "In China 100 million people access the Web through Internet cafes. For them it is not about downloading, it is about the experience. In the US it is still all about ownership" (Frater 2005).

Projects like Microsoft's Venus operating system have focussed on dramatically lowering the cost of accessing the internet from home, a move which would help bring millions of previously isolated consumers into the digital realm. Venus is designed to allow a web browser, a low end personal computer and a video compact disc player to be combined in a single box that can be used in conjunction with a television, for people who cannot afford a traditional PC (Reuters 1999). Another, more recent development is Internet Protocol Television (IPTV; cf. sources), which allows television or video signals to be distributed over broadband, using Internet protocols. Telecommunications providers are also looking towards IPTV as one of the next major developments in content delivery in China. Rapidly rising rates of broadband penetration and the launch of IPTV services by Internet service providers will undoubtedly create new opportunities for digital content providers. According to IDC, although there are expected to be less than 300,000 IPTV subscribers in China by the end of 2005, this figure is expected to reach 9 million by 2008 (Le Maistre and Newlands 2005).

Mobile devices and services

China has experienced enormous growth in mobile phone uptake over the past five years. Each month about 5 million people sign up for mobile services for the first time (Kessler 2004). Saturation of the handset market is prompting the industry to focus on handset upgrades and value added services. Mobile technology companies predict that overall growth in the market will continue, and expect to see sharp increases in demand for mobile content as 3G networks expand and the content becomes more affordable.

Mobile phones are already providing an important revenue stream for Chinese record labels. Consumers are paying for mobile ringtones (*cai ling*) and ringback tones and copyright owners have had some success in ensuring that they receive a portion of the money being spent on these services (Montgomery 2005a, c, d). Many record industry players see mobile content as key to the future of China's music industry (Montgomery 2005b, c, d, e). Chinese consumers are spending a high proportion of their income on mobile telephones, accessories, and content required to personalise them.

In contrast to the slow development of online MP3 sales, two important factors are making it possible for a copyright compliant mobile music market to emerge. These are

1) An established billing system; and

2) The ability to control the distribution of mobile phone content through a limited number of mobile service providers.

The cost of mobile content services is simply added to each customer's monthly bill

(Montgomery 2005a). Mobile service providers are responsible for collecting payments and passing royalties (or a negotiated fixed amount) on to copyright owners.

Legal protection for copyright owners and user rights

Membership of the World Trade Organisation requires China to enforce its domestic intellectual property laws and to meet the obligations relating to copyright protection set out in the agreement on Trade Related Aspects of Intellectual Property (TRIPS). China has been involved in a steady process of copyright reform in accordance with international practice since the 1980s (Qu 2002). In November 2001, as a result of joining the World Trade Organisation, the government approved amendments that brought China more closely into line with TRIPS and the Berne Convention (Fitzgerald and Montgomery 2005).

Anti-circumvention provisions

Technical protection measures put into place by the copyright owner are explicitly protected under Article 47 of the Chinese copyright law (1990). Civil and administrative remedies are available for any act of intentionally circumventing and damaging protection measures put into place by the copyright owner, and for deliberately deleting or altering electronic rights management information, without the copyright owner's consent (Fitzgerald and Montgomery 2005).

Moral rights

Authors have a right to be acknowledged for their efforts (a right of attribution) and a right to be consulted in relation to any changes made to their work (rights to alteration and integrity) for an unlimited period. These rights exist separately from the economic rights associated with copyright, and continue to belong to the author even after the exploitation rights have been sold on. Copyright is protected for the life of the author plus fifty years. Works created by corporations or other entities are protected for fifty years, as are cinematographic, film or photographic, television or audiovisual broadcast radio and television programs (Fitzgerald and Montgomery 2005).

Fair use

China's copyright law provides extensive fair use exceptions, including for "private study, research or self-entertainment". Nonetheless, copyright owners do have legal protection against sites providing music downloads without payment to or permission from the copyright owner. In addition to the anti-circumvention provision of the law, it is an offence to reproduce or distribute a product of sound or video recording, or to make it available to the public through an information network, without the permission of the producer.

Legal remedies

According to articles 46, 47, 49 and 50 of the copyright law, victims of copyright infringement can seek civil and administrative remedies, including monetary damages, injunctions, public apology and destruction of offending products. The onus of proof rests with alleged infringers.The copyright law requires infringers to pay compensation according to the actual injury inflicted on the copyright owner by the infringing act, or according to the profits derived from the infringing work. In cases in which it is difficult to establish the right holder's actual injury or the infringer's unlawful income, the courts may award statutory damages of up to 50,000 RMB (approximately US $6,200). China's 1997 Criminal Law also provides penalties of up to seven years imprisonment for copyright related offences.

Three channels for copyright enforcement exist in China: Civil, Administrative and Criminal. Civil action requires parties to take action on their own behalf, through the courts, in response to infringement of their rights. Administrative action is taken by the Administrative Department for Copyright directly, rather than through the courts. Prosecution of criminal actions can only be undertaken by the state. This means that, in addition to civil action, copyright owners also have the choice of working with the copyright department directly in order to stop infringement. The Copyright Department has the power to issue injunctions, confiscate unlawful gains, confiscate and destroy infringing material and the tools used to create them, and to issue fines to punish infringers.

However, while administrative authorities have the power to impose fines, only the courts have the power to require infringers to pay compensation to copyright owners.

Discussing the role of DRM and alternatives

The biggest challenge for Digital Rights Management in China is the availability of un-protected content. It is unrealistic to expect users to pay for content that carries restrictions relating to the ways in which it can be copied, shared and re-distributed while unrestricted versions of the same material are available for free elsewhere.

Current levels of piracy are forcing copyright owners in China to develop business models that take into account the distribution environment. Major record labels originally attempted to charge Chinese audiences prices for CDs comparable to those demanded in markets such as the US and Australia. However, since 2003, all of the major labels have lowered their prices in an attempt to compete with pirated products (Montgomery 2005c, d, a). Advertising, product endorsements and sponsorship are also being pursued as important strategies to generate revenue streams.

Ring tone downloads and ring back tones are arguably more significant as a source of income for many Chinese music industry players than royalties from album sales. Artist management services, which allow record labels to capitalise on advertising, publicity and concert fees generated by their stars, are also much more significant in the Chinese music industry than they are in markets where intellectual property rights are easier to enforce.

In this environment, new technology, which can be engineered with controlled distribution in mind, will play an important role in China, where existing media formats, such as cassettes and CDs, are already established as the centre of a massive industry of unregulated distribution. It is highly unlikely that the genie can be put back into the bottle when it comes to established piracy networks. Nonetheless, technological developments that force content to pass through a limited number of regulated portals may help to secure new income streams in the future.

The success of mobile content services in an environment where most copyright owners are struggling to realise the value of their intellectual property may provide lessons for the sector more generally. The fact that consumers have no choice but to purchase mobile services from a restricted number of mobile providers makes it possible, for the most part, for copyright owners to monitor the distribution of their products. It is conceivable that similar arrangements with IPTV service providers may help to resolve some of the problems associated with micro payment for online content as the sector develops.

Greater transparency and accountability within China's group collection agencies, as well as among internet service providers and search engines will also be crucial to realising the potential of China's copyright industries. The availability of illegal online content cannot be controlled without such changes. But reducing the availability of free online content will not be enough. China's copyright owners will also have to ensure that legitimate content is available quickly, conveniently and easily to consumers when they want it. The impact of DRM measures on the attractiveness of the content being offered will need to be considered in the context of this supply/demand equation.

Bottom line

It is possible that the copyright environment in China may force intellectual property owners to move away from a royalty-based system for content provision. Advertising is already playing a vital role in generating music industry income. It may be necessary for record labels to consider an integrated business model, in which content is given away online, in exchange for audience numbers and willingness to purchase mobile content services, merchandise, tickets to live performances and other associated products. It may be time for China's music industry to accept that the intrinsic value of their products lies in the ability to attract audiences, to entertain, and to spark an interest in purchasing associated services. Consumers who are

used to receiving content for free will not willingly shift to a system which expects them to pay. This will be particularly true if the products they are asked to purchase are rendered less attractive and convenient to use by DRM restrictions.

Sources

- BBC (2004): PC ownership to 'double by 2010'. BBC News Online; http://news.bbc.co.uk/1/hi/technology/4095737.stm
- China Economic Review (2005): Baidu will appeal guilty verdict. China Economic Review; http://www.chinaeconomicreview.com/subscriber/newsdetail.php?id=6095
- CNNIC (2005): 16th Statistical Survey Report on the Internet Development in China; http://www.cnnic.cn/download/2005/2005072601.pdf
- Copyright Law of the People's Republic of China (1990)
- Fitzgerald, B. and A. Montgomery (2005): Copyright and the Creative Industries in China. Innovation and Creativity In China (ICIC) Conference, Beijing
- Frater, P. (2005): Soundbuzz opening Asia digital boom box; http://www.variety.com/article/VR1117927002?categoryid=16&cs=1&s=h&p=0
- IPTV: http://wn.wikipedia.org/wiki/IPTV
- Kessler, M. (2004): US Firms Doing Business in China: Tough but Critical; http://www.usatoday.com/money/world/2004-08-17-china-tech_x.htm
- Le Maistre, R. and Newlands, M. (2005): China Shapes Up for IPTV Boom; http://www.lightreading.com/document.asp?doc_id=73529&print=true
- Montgomery, L. (2005a): Interview with Beaker Huang, Artist Manager and BD Director, Warner Music China: 13
- Montgomery, L. (2005b): Interview with Shan Qi, Central China Television, Artist Life, Traditional Opera and Music Department
- Montgomery, L. (2005c): Interview with Simon Chu, Senior Vice President, National Division, Universal Music Limited, Hong Kong
- Montgomery, L. (2005d): Interview with Song Ke, Managing Director, Taihe Media and Music Entertainment Company Limited. Beijing
- Montgomery, L. (2005e): Interview with Zhou Yao Ping, Beijing Birdman Entertainment Company. Beijing
- Qu, S. (2002): Chinese Copyright Law. Beijing, Foreign Languages Press
- Reardon, M. (2005): China to Trump US in Broadband Subscribers; http://news.com.com/China+to+trump+U.S.+in+broadband+subscribers/2100-1034_3-5695591.html
- Reuters (1999): Microsoft: Cheap Net for China. Wired News; http://www.wired.com/news/print/0,1294,18373,00.html

About the author: *Anna-Lucille* (Lucy) Montgomery is a doctoral candidate and researcher at Queensland University of Technology's Creative Industries Research and Applications Centre. She is currently completing the final year of her PhD, titled: Copyright, Creativity and Economic Development: Intellectual Property and the Creative Industries in Post-WTO China. E-mail: a.montgomery@qut.edu.au

Status: first posted 29/09/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=141

Online music in Hungary

By: Kristóf Kerényi, SEARCH laboratory, Budapest, Hungary

Abstract: For legal reasons, and also because of the smaller and less substantial market, big players of today's online music are not active in Eastern-Europe. The author takes the example of Hungary and introduces the current situation and difficulties when buying digital music online, from the consumer's point of view. Lack of competition causes high prices and low level of service, the combination of which favours unofficial and illegal sources of digital content.

Keywords: hands-on-experience – consumer expectations, music markets – Hungary

Introduction

On 26 August T-Mobile Hungary, the Hungarian subsidiary of Germany's global telecommunication provider announced the official launch of its 3G mobile network (cf. sources). Not that there hadn't been 3G mobile services before in Hungary, it's only that these were not yet "official". Both of the other two mobile operators, Pannon GSM (owned by Telenor, Norway's largest telecommunications group) and Vodafone Hungary have their own "experimental" 3G networks, meaning that in many cases consumers can use these networks for free, and they can experiment with the new line of services (video conferencing, mobile TV, fast data communication). Of course when one wants to promote the new, faster generation of mobile access (together with the higher rates), adequate services running on it are also needed. So T-Mobile – in the same press release – also announced a new music download service.

On the same day, I read a rather negative review of the service (Ady 2005). So, having tried music downloading in Hungary before, I decided to take a look at the market, and write an objective, and at the same time very opinionated review of what choices a Hungarian person has to obtain digital music from the "network". Thus I am looking at the situation as a consumer, and will come to the conclusion that in our country today legal download services are just not an option.

A game with few players

A year and a half ago, in April 2004 Hungary's first paid music download service, "Origo Play" was launched by a company named Axelero, the ISP owned by the Hungarian national telecom company (today T-Com). So I gave it a try earlier this year, just to experience the feeling of paying for downloading music. I also wanted to write an article about it, but my experience was so scarce and disappointing that it would have rather been a complaint.

Last week I tried to find all "official" music download services available here, but there were only three of them. I also tried to gather information at the Hungarian Bureau for the Protection of Authors' Rights, because they must know about all of these, but I was a bit disappointed to learn that there are just a few players on the market.

Starting from the back, they directed me to some sites which already have their permission but haven't started their service yet; there are also radio stations (among them the Hungarian Radio) that make past broadcasts, and musical programs available for downloading, among them in many cases real "treasures": old recordings and rarities (cf. sources). However, none of them is a paid service and, as a consequence, they are not DRM-protected. Some make available their downloads in unprotected Real Audio format, others use the free OGG Vorbis format.

I also took a look at the three Hungarian mobile service providers: Vodafone, in spite of being the biggest European operator, currently does not have a music download service in Hungary (however, as I learned they have a licence to start it), the other two have almost identical services and pricing (cf. sources).

With one Internet-based offer available to everyone (the mobile operators' services are just for their own subscribers) this makes three options, which do not even compete, since mobile phone subscribers usually do not decide on the basis of the available music services…

The single Internet offer

Every day we hear about the success of internet music download services: iTunes, Connect, MSN, Real and Yahoo are just a few examples, so one might think that we have a huge selection to choose from. The sad truth is that because of legal issues and distribution agreements with the labels none of the mentioned services are available in Hungary. So we have to stick with the only Hungarian download service, which is operated by the local branch of T-Online (cf. sources).

At least this service can be tried by everyone… Well, not exactly everyone, just those who use Windows, and a compatible portable player, since this music store uses Microsoft DRM. Otherwise the whole purchasing process is quite fine. They have a user- friendly interface, lots of information on the used technology, also on DRM, what can and cannot be done with the tracks, and so on. The selection can be searched by title, band or album, or one may just browse by genre. The only problem is that *this meta-information* is completely messed up (e.g. Pantera (Metal) and Adam F (Drum & Bass) are both classified as Pop, *Bódy Magdi* (mostly Jazz) is classified as Soul). As I mentioned already, I decided to try it just for the feeling. I was looking for something that I like, and interestingly I did not find such songs easily in the selection. Alright, I have a little bit nonconformist musical taste, so this didn't really disturb me. Since then I have visited the music store a number of times and I found out that *there are* bands that I like, I just do not find them easily. And now with a decent line of history I would expect at least some personalized offers like "users who bought this liked those too" – like in the "big" stores. By the way, the selection consists of 130,000 songs, and is continuously growing. However, as I mentioned, important meta-information is missing, or false. Therefore one of the main advantages of music stores, namely *information* (Kerényi 2004), does not apply here.

When we have already found what we would like, we can listen to the first minute of the track to decide whether this is really the desired song. Of course this first minute comes in very low quality so that no one has the idea of grabbing it. The full track, when purchased, comes in 160 kbits/second WMA format, which *would* be enough for everything, but alas!, some tracks are distorted! (We do not even have to turn up the volume; the peak of the bassline is cut off.). Bad luck for those who think *this is digital music*.

The pricing is quite interesting: the "average track" goes for (a little over) € 1, but some tracks go for € 1.4. For what reason, I do not know, I didn't find a correlation. For this amount of money we receive at most two "licences" (this means the tracks are playable on two computers), but at least they are transferable to an unlimited number of portable players. For the number of CD burns, however, there is no general rule, it is determined on a track-by-track basis. I couldn't find a lower number than two or a larger number than ten. I didn't find differences within an album, but there could be, since the terms and conditions say that the user is responsible for checking this *for each track*. Very consumer-friendly rules, I must say.

Mobile music

It makes sense to compare the two mobile service providers' music download offerings, because they share the restrictions of the mobile platform, and also because they have similar pricing.

Pannon GSM, which started its service as the first player is a customer of Groove Mobile, an American company which delivers downloadable music to three continents. They licence music from Warner, Universal, Sony, EMI, BMG, V2, and lately also Beggars Group, which is the home of a number of UK independent labels (cf. sources). However, not every label's offerings are valid in every country, so Pannon's subscrib-

ers can only access "tens of thousands" of songs, paying € 1.6 for each (cf. sources).

T-Mobile has a very similar system (at least on the phone it looks similar) to the aforementioned, but I could not find information on where they license the music from. However, they offer 300,000 songs, so the point goes to T-Mobile in this respect; but not in pricing, they charge € 2.1 for a track.

Both providers use a proprietary DRM solution, for which a freely downloadable program is used that runs only on Symbian operating system-based smart phones. The first such phone appeared around two years ago, and both Nokia and Sony Ericsson are continuing their line with the newest 3G phones. Pannon GSM describes most such phones on the market as supported, while T-Mobile lists only the two newest 3G phones from Nokia as being capable of running the DRM framework. The question is, if the technology used in the new 3G phones is identical to that used in the other Nokia phones, why does the program not support other Nokia models, like their competitor's?

Pannon GSM writes on its web page that the DRM of the downloaded track is bound to the SIM of the phone, meaning that if we transfer the tracks to another phone *and* replace the original SIM, the songs will play on the new device. T-Mobile only says that the songs will only play on one's "own mobile phone", so the tracks can be backed up to an external medium, but will only play on the "own device". This means that neither of the two supports transferring and playing the songs on a PC. The question arising here is that if all of the supported phones are compatible with the OMA DRM standard, why not use OMA DRM? If both companies used the OMA technology, they could be compatible with more devices (meaning a bigger market) and perhaps also with each other (meaning bigger competition). But perhaps this is not their aim…

Both companies provide a 30 seconds prelistening of the tracks. The tracks are downloaded in AAC format, and – according to the information available on the internet – normally use 700-900 Kbytes from the memory of the phone. After a little bit of counting (1.15 Mbytes for 4m48s: 1150*8/288) this means a bitrate of 32 kbits/second , which results in low sound quality, even in the efficient AAC format – by the way this is the same as the low-quality prelistening bitrate of the aforementioned Internet-based music store. At least the double would be needed to produce enjoyable music pieces, and four times this for CD quality (iTunes also uses 128 kbits/second encoding).

We should also mention download costs. Now that the high-bandwidth 3G networks are in their experimental or early commercial state, network traffic over them is for free, but only for a limited time. However, even in the bigger cities of Hungary we are still very far from decent UMTS coverage. So, if one wants to use the mentioned download services, in most cases one will have to go back to the traditional GPRS/EDGE networks, where browsing and downloading costs can easily double the price of one track, since in Hungary data traffic is not included in the price of the songs.

Ringtones

We can also consider mobile phone ringtones as a kind of digital music, particularly for the latest mobile phones, where pieces of music sound in excellent quality when the phone rings. There are approximately 50 such licences in Hungary this means that around 50 providers may sell musical ringtones. So we can assume that ringtones make up the majority of online music sales. Though I personally do not consider these online music downloads, since they are usually not whole tracks, I think it is worth seeing how much they cost.

Normal polyphonic MIDI ringtones usually cost around € 1.2, better quality, so-called "True Tone" ringing effects (i.e. non musical, e.g. animal voices and other effects) cost around € 1.6, and interestingly "True Tone" music ringtones (copyrighted material) cost € 1.9. So here we can see that there is an extra charge built into music over effects. There is also the possibility of downloading true music tracks as ringtones. Here the charge from each mobile provider is € 2.4, even more than for a whole song!

Conclusion

Summing up the experiences gained: on the mobile market the consumer has to pay up to € 4 for a track that he can only listen to on one phone and nowhere else. And in many cases the sound quality of the purchased music is worse than that of a ringtone. But those people, who are willing to pay € 2.4 for a ringtone, may find this offer tempting…

On the Internet music market, today's single Hungarian player without any competition sells songs for more than in almost any richer European country and with stricter conditions. The quality of the music is not flawless either, and the information service provided also leaves things to be desired.

We expect that online music is just taking off in Hungary and in the next half year many new providers will enter the market. I am curious.

Bottom line

My experiences of the Hungarian online music market are distressful, and the sad thing is that the same probably holds for the rest of Eastern-Europe, meaning at least 75 million people. Prices are sky high, and quality of service does not even come close to the desired level. With affordable broadband internet access everywhere and no real alternative, file-sharing and illegal music and video downloading rule the scene. DRM-based services will have to become a lot better to beat the free offerings of the (dark)net.

Sources

- Ady, Krisztián (2005): T-Mobile has started a mobile music store. HWSW IT magazine, 26/08/2005, http://www.hwsw.hu/hir.php3?id=29652&count16=1
- Groove Mobile (2005): http://www.groovemobile.net
- Hungarian Radio (2005): http://www.radio.hu
- Kerényi, Kristóf (2004): DRM strategies debate in the US – A report from a JupiterMedia Conference. INDICARE Monitor, Vol. 1, No 6/7, December 2004; http://www.indicare.org/tiki-read_article.php?articleId=65
- Pannon GSM (2005): http://www.pannongsm.hu
- T-Mobile Hungary (2005): http://www.t-mobile.hu
- T-Online Music Store (2005): http://zenearuhaz.t-online.hu
- Vodafone Hungary (2005): http://www.vodafone.hu

About the author: *Kristóf Kerényi* is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His interests include mobile and wireless IT security, as well as technological aspects of DRM. He received a MSc in computer science from BUTE. Contact: kerenyi@mit.bme.hu

Status: first posted 26/09/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=138

Popkomm 2005: DRM not in the focus

By: Nicole Dufft, Berlecon Research, Berlin, Germany

Abstract: The music fair Popkomm took place between September 14 –16, 2005 in Berlin. DRM played a less prominent role as a stand-alone topic than last year. One important focus this year was on new digital business models, such as mobile music, podcasting and other new radio formats, or subscriptions. This article gives a short impression of the discussions on this year's music fair.

Keywords: conference report – business models, music industry, music markets, podcasting

Introduction

For 17 years now the Popkomm has been one of the most important fairs for the music industry worldwide. This year, 796 exhibitors – 130 more than last year – from 49 countries attended the event in Berlin. The future for the music industry today looks a bit brighter than in previous years. According to *Gerd Gebhard*, chair of the German IFPI (Federation of the Phonographic Industry), particularly online music services show a promising development and the music industry is embracing the digital age by testing new music formats and pricing models. Naturally, Gebhard could not refrain from touching the issue of music piracy as well.

No dedicated DRM sessions at this year's Popkomm conference

Each year, the Popkomm music fair is accompanied by a rich conference program, where new developments in the music industry are discussed with top-level experts. As opposed to the Popkomm conference in 2004 (cf. Dufft 2004), no dedicated DRM session was on the agenda of the conference this year. Naturally, DRM is an important foundation for many of the discussed new business models. It therefore played a role in the discussions, but less prominent than in the previous year.

Big hope put on mobile music

One session of the conference was dedicated to mobile music. Music labels, mobile operators and device manufacturers all expect – or rather: hope – that music on mobile phones will become a soaring new source of revenue. However, incompatible file formats and DRM technologies as well as problems with providing downloads that can be used in parallel on PC and mobile phones constitute important limitations for the future success of full-track music downloads. Patent problems were also mentioned, especially concerning the OMA DRM standard (cf. on this topic Bohn 2005).

Subscriptions versus a-la-carte downloads

The future success of a la carte downloads and subscription services was discussed in a dedicated digital music session. It was conceived that subscription services should gain considerable attention also in Europe, where adoption is yet slow compared to the US. Adequate pricing models for music subscription services were discussed in detail. Low-price offerings, in particular Yahoo! Music Unlimited, which offers a subscription for only $ 5 per month to US clients, might force the involved players to accept shrinking margins. *Dave Goldberg*, Vice President & General Manager of Yahoo! Music provided for an interesting insight of Yahoo's strategic goals: while in retail markets prices usually start high and decrease over time, the opposite could be true for services markets, e.g. subscription services. Spelled out this means that Yahoo will try to lock in as many customers as possible and then gradually increase prices for the service over time.

Who kills the radio star?

A session called "New radio" focussed on new radio-like services, such as Web radio, mobile streaming services and podcasting. A first panel discussed the new business models. It was stressed that a whole range of new revenue sources and a range of different

players now dominate the music business, e.g. ISPs and operators selling broadband and mobile network traffic, or technology companies selling devices and software. However, for a number of very popular music services such as Web radio or podcasting, profitable business models have not yet been developed. A second panel focussed on what the new digital services mean for traditional radio broadcasters. Music consumption has over the past years increasingly become an active process, where consumers choose what they want to hear on the device, at the place and at the time they like. Traditional radio broadcasters have to respond to this development, e.g. by offering their own podcasts or web streams and by offering high-quality programs, not only mainstream music that sounds all alike.

Is podcasting sexy?

On the last day of Popkomm a session named "Podcasting is sexy" explicitly dealt with this new form of radio-on-demand. Podcasting was a "hot" topic discussed in many other sessions as well. Open copyright and licensing issues for musical content, however, currently limit the broader adoption of podcasting (cf. on this topic Dufft 2005). Nevertheless, some market participants like the BBC see high potential in podcasts, and major labels slowly start to take the new medium seriously. Warner Music, for example, produces its own podcasts and provides samples of its music to be used in podcasts.

Bottom line

DRM by itself was less intensively discussed on this year's Popkomm than last year. However, my impression was that the music industry is becoming more creative and innovative to develop and test new business models that serve the specific demands of consumers. In this environment DRM is "simply" a technical problem that needs to be solved properly. It is not anymore regarded as a key element that will shape the future of digital business models. Rather, the diversity of consumer tastes, not only concerning different music genres but also concerning different consumption behaviours is coming more into focus – finally.

Sources

- Bohn, Philipp (2005): Mobile DRM convergence, INDICARE Monitor, Vol. 2, No 6, August 2005, http://www.indicare.org/tiki-read_article.php?articleId=135
- Dufft, Nicole (2004): The music came to Berlin: Popkomm 2004. INDICARE Monitor, Vol. 1, No 5, October 2004; http://www.indicare.org/tiki-read_article.php?articleId=51
- Dufft, Nicole (2005): Podcasting-profit-possibilities. Will DRM invade the scene?, INDICARE Monitor, Vol. 2, No 5, July 2005, http://www.indicare.org/tiki-read_article.php?articleId=122
- Popkomm Website: http://www.popkomm.de

About the author: *Nicole Dufft* is a senior analyst at Berlecon Research. She has been analysing a variety of ICT topics ranging from mobile computing and application service providing to DRM. Currently, she works in the field "digital consumer". She is a member of the INDICARE project team. Contact: nd@berlecon.de

Status: first posted 30/09/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=144

Improving cross border licensing practices for online music stores

The European Commission's view

By: Margreet Groenenboom, IViR, Amsterdam, The Netherlands,

Abstract: On 7 July 2005, the European Commission released the staff working document "Study on a community initiative on the cross border collective management of copyright" (European Commission 2005a). This article reviews the aforementioned Study, focusing on the current difficulties in the licensing of online music, solutions that were brought forward by the industry (for instance the Santiago Agreement), the policy options proposed by the European Commission and the influence of DRM on collecting societies.

Keywords: review – collecting societies, competition, DRMS, licensing contracts, Santiago agreement – EU

Introduction

The aim of the "Study on a community initiative on the cross border collective management of copyright" (Commission staff 2005, "the Study") is first to identify the problems related to the current structures for cross border management of copyright for online content services, and secondly, to propose possible solutions to improve the current situation. At the time of writing, 80 organizations and other stakeholders had already submitted their reactions on the Study to the European Commission (Contributions 2005). In the first half of 2006, the European Commission will conduct an impact assessment on recasting copyright. The results of this assessment are expected in the second half of 2006 and there could be a first policy debate on the cross border management of copyright in the fall of 2006. This article will only address the Study, not the reactions to the Study. The 60-page Study consists of 7 chapters:

1. Problem definition;
2. Objectives;
3. Policy options;
4. Analysis of impacts;
5. Monitoring and evaluation;
6. Results of stakeholder consultation and
7. Commission proposal and justification.

Explaining the problem

Before addressing the content of the Study, a brief introduction to the problem will be given. Collecting societies in the EU Member States are based on a state endorsed monopoly. A collecting society in a certain Member State enforces exploitation rights of rightholders (copyright owners) based in that same Member State by granting licenses to commercial users. The collecting societies can endorse these rights without the explicit permission of rightholders. In addition, they audit and monitor rights by ensuring payment and terms of licensing. After the collection of the royalties, the collecting societies distribute the royalties to rightholders. The distribution of royalties is especially complicated when it concerns cross border management. When someone, for instance an online music store, wants to offer music, he would have to conclude agreements with the individual collecting societies in all the countries where it intends to offer music.

The above mentioned practice of concluding a license in each and every EU Member State with the local collecting society for 1 song, leads according to the Study to difficulties for online music services to start their business. The Study defines online music services as any music service provided on the Internet or provided to mobile phones. Examples are services such as simulcasting, webcasting, streaming, downloading, and online "on-demand service". The Study uses the estimate by the European Digital Media Association – an organisation representing online music providers – in determining the direct costs of licensing a song. The negotia-

tion of one single license (mechanical and public performance rights) would cost 19,000 Euro. When clearance for a song is required in all 25 EU Member States, this would amount to 475,000 Euro. On the basis of a profit of 0.10 Euro per download, 4.75 million downloads are required to cover the costs of the license.

Also, in comparison to the situation in the United States, the licensing of online music in the EU is far behind, at least according to the Study. Where in the United States 207 Million Euros were spent on music downloads, only 27.2 Million Euros had been spent in Europe.

The problem can be illustrated by using iTunes as an example. Imagine a song being offered by iTunes-UK. A consumer, living in the Netherlands, wants to purchase the same song from iTunes- the Netherlands. The song is not available and he wants to purchase it from iTunes- UK. This is not possible though! In this case, there obviously is no license to sell the song in the Netherlands. For each country where Apple aims to sell the song, a separate license is required.

Some findings of the European Commission

The Study identifies in Chapter 1 three categories of restrictions which hinder the licensing of online music. First, restrictions exist with regard to cross border licensing. At the moment, there is no universally acceptable multi-territorial agreement for the online rights of all categories of rightholders. Secondly, restrictions exist with regard to the cross border distribution of royalties. For example, collecting societies do not provide for non-discriminatory distribution for rightholders from all EU Member States. Thirdly, a restriction is formed by the Santiago and the BIEM/Barcelona Agreements (Santiago Agreement 2001 and BIEM / Barcelona Agreements 2002) which oblige content providers to go to the collecting society in their own Member State (this is called the economic residency clause). Because the Santiago Agreement forms an important part of the Study, we will have a closer look at this Agreement.

Santiago Agreement

The Santiago Agreement authorises collecting societies to grant non-exclusive licenses for the online public performance of musical works (songs) on a worldwide (multi-territorial) basis to content providers. On 29 April 2004 the European Commission notified the sixteen European collecting societies that entered this agreement, that the *Most Favoured Nation clause* and the "economic residency clause" in the Santiago Agreement may violate European Union Competition law (European Commission 2004). The "economic residency clause" enforces section II of the Santiago Agreement in which is determined that the collecting society with authority to grant multi-territorial licenses, is the society of the country where the content provider – for example an online music store – has its actual and economic location. As a result, each national collecting society is given absolute exclusivity for its territory with regard to the possibility of granting multi-territorial licenses for online music rights. Although the Santiago Agreement aims to promote the use of "one-stop shop" copyright licenses, the result is thus a lock up of national territories which might constitute a breach of Article 81 EC Treaty. Article 81 EC Treaty prohibits all agreements between undertakings, decisions by associations of concerned undertakings and concerted practices which may affect trade between Member States and which have as their object or the effect the prevention, restriction or distortion of competition within the common market. In this Study, the European Commission tries to propose a solution, which would not violate Article 81 EC Treaty, for the granting of a world-wide license for a song to online music stores by one central collecting society.

Digital Rights Management

Separately, attention is paid by the Study to Digital Rights Management (DRM) (see for example chapter 1.2.2). Digital technologies in rights management have empowered rightholders to control the licensing by the facilitating of and tracking the use of works. Examples of facilities enabled by the use of a DRM system are individual electronic payment and remote monitoring. Because DRM

enables rightholders to license their rights themselves they do not necessarily need collecting societies to take care of this issue. Therefore, collecting societies should assess the services they currently offer rightholders and decide which services are of surplus value to rightholders. Using digital technologies might also lead to a reduction in management costs for collecting societies and will enable them to be more accurate in royalty distribution. In the INDICARE-interview with A. Beemsterboer of CEDAR, Beemsterboer elaborated on the possibility of collecting societies using DRM. As an example of a new service to rightholders, Beemsterboer envisaged the collecting society as a broker in licenses (Helberger 2004). By using DRMs, the collecting societies could be adapted to the digital environment. Lastly, digital technologies could allow collecting societies to outsource some of their management services when this is more efficient than providing these services themselves.

General policy objectives

The "opening up of Europe's large and mainly underexploited potential of growth in legitimate online services" forms the general policy objective identified in Chapter 2. More specifically, the accessibility of creative output especially to online content providers should be improved and there should be a full participation of rightholders in the revenue stream generated by more efficient cross border exploitation of copyright. In order to achieve these objectives, the Study proposes the following operational objectives:

- A licensing policy that is in line with the demand of online content providers;
- Transparency of collecting societies;
- Improved copyright clearance of copyrighted works across the EU;
- A significant increase in the availability of multi-territorial licenses for online content providers;
- Freedom for right holders to choose their collecting societies and to have the ability to switch between collecting societies;
- Enhancement of transparency and accountability of collecting societies and equitable distribution and enforcement of rights;
- Distribution of royalties collected on behalf of the rightholders in territories other than their home territory to rightholders directly and without discrimination on the grounds of residence, nationality or category of membership.

In addition to these operational objectives, the Study proposes in Chapter 5 indicators to monitor and evaluate the developments.

Policy options, analysis of impacts, the Commission's proposal and its justification

The European Commission considers three options to improve the current situation in Chapter 3:

- Option 1: Do nothing;
- Option 2: Suggest ways in which cross-border co-operation between national collecting societies in the 25 Member States can be improved;
- Option 3: Give rightholders the choice to authorise one single collecting society to license and monitor all the different uses made of their works across the entire EU.

The European Commission analyses the three policy options for different aspects (for instance legal certainty, transparency, innovation and growth, competition and the impact on specific groups) in Chapter 4. Although option 2 would improve the way reciprocal agreements function, it will not remove limitations contained in these agreements and there will be no scope for collecting societies to improve their services or differentiate their repertoire. Following option 1 and 2 would – according to the Study – have the consequence that rightholders still need to go to the collecting society of their own EU Member State and do not have any choice at all. Option 3 though, would give rightholders the opportunity to authorise a collecting society of their choice to manage their works across the entire EU. The Study expects that competition between collecting societies will create a competitive environment for cross border management of copyright in which collecting societies will pro-

vide better services to rightholders, for instance the improvement of cross border royalty payments and the specialisation in genre-specific repertoires.

Consultation of stakeholders
In drafting this Study, the European Commission made use of a stakeholder consultation (see Chapter 6). It appears that rightholders and their representatives focus on improving the cross border distribution of royalties. Commercial users focus more on the community wide licensing process. With regard to the last issue, opinions from stakeholders differ. The Groupement Europeen des societies d'auteurs et compositeurs favours a community wide license given by the collecting society in the territory where the online operator has its economic residence. The Association of European Radios, MTV Networks, European Information & Communications Technology Industry Association and some online content providers favour the freedom for users to choose between collecting societies. The Music Publishers Association is against competition and free choice with respect to a single licensor, as this would permit users to engage in "perpetual negotiations" with several competing collecting societies.

Implementation of the policy
In order to realise the identified general policy objectives, the European Commission suggests (in Chapter 7) a series of core principles that EU Member States should adhere to, e.g.:

- Rightholders' choice as to the online management society is based on the freedom to provide rights management services directly across borders. The freedom to provide cross-border management services by means of direct membership contracts will eliminate administrative costs inherent in channelling non-domestic rightholders royalties through reciprocal agreements between different societies;
- The principle that a rightholder's choice of a single EU rights manager should be exercised irrespective of residence or nationality of either the rights-manager or the rightholder;
- The principle that a collective rights society's repertoire and territorial licensing power would not derive from reciprocal agreements but from rightholders concluding contractual agreements directly with a society of their choice. Rightholders should be able to withdraw certain categories of rights (in particular categories of rights linked to online exploitation) from their national collecting societies and transfer their administration to a single rights manager of their choice. For that to work, these online rights must be withdrawn from the scope of reciprocal agreements as well;
- The principle that the individual membership contract will allow the rightholder to precisely define the categories of rights administered and the territorial scope of the society's authority. As the licensing authority would derive from the individual membership contract, the collective rights manager of choice would not be limited to managing these rights in his home territory only, but throughout the EU;
- Individual membership contracts create a fiduciary duty between the collecting society and its members, obliging the former to distribute royalties in an equitable manner. The principle of equitable distribution obliges collecting societies to treat domestic and non-domestic members alike with respect to all elements of the management service provided. The fiduciary duty enshrined in membership contracts is thus is a tool to maximise the royalties that accrue to rightholders;
- Membership cannot be refused to individual categories of rightholders who represent mainly non-domestic interests (e.g., music publishers). In addition, these rightholders should have a voice in how royalties are distributed that is that is commensurate to the economic value of the rights they represent;
- Non-discrimination as to the service provided and the fiduciary duty of the collective rights manager vis-à-vis its members introduces a culture of transparency and good governance as to how

rights are collectively managed across EU borders.

A bit of discussion

Although the European Commission analyses different aspects of the three policy options, it seems that the European Commission considers the following as most important aspect: the opportunity offered by option 3 for rightholders to authorise a collecting society of their choice to manage their works across the entire EU. When taking into account the objectives identified before, the choice made by the European Commission for option 3 is logical. The results of the stakeholder consultation - concerning the cross border distribution of royalties - do not necessarily point to the adoption of policy option 3 though. Improvements in this field might also be enabled by implementing option 2. With regard to community wide licensing, some stakeholders quoted in the Study seem to favour the freedom to choose between collecting societies. Whether this is indeed true can only be established by assessing the stakeholders' reactions to the Study.

Recently, the collecting societies BUMA (the Netherlands) and SABAM (Belgium) announced that they will not be party "to any agreement on licensing of public performance rights for online use with other copyright management societies containing an economic residency clause, similar to that contained in the Santiago Agreement and identified as restrictive in the Statement of Objectives" (BUMA/SABAM 2005 and European Commission 2005b). This might be an indicator that some collecting societies do indeed favour the policy option chosen by the European Commission.

Conclusion

Overall, the Study is well structured and when analysing the policy options it takes into account many different aspects, ranging from legal certainty to the impact on specific groups. The problem definition makes it clear that something needs to be done soon to make the community wide licensing of musical works easier. When analysing the policy options, the European Commission considers DRM to play the largest role in fulfilling policy option 3. More specifically, DRM could improve the services offered by collecting societies. Because DRM enables rightholders to license works directly to commercial users, collecting societies should consider the surplus value of their services to keep rightholders interested in their services. Maybe they should consider offering new services, see for example the "broker in licenses" service suggested by Beemsterboer. Furthermore, the use of DRM by collecting societies could enhance the cost-efficiency within collecting societies.

Bottom line

The proposed policy options and the analysis of impacts in the Study have certainly triggered stakeholders to react and to continue the debate in this field. I am looking forward to the assessment of the reactions!

Sources

- BIEM/Barcelona Agreements (2002): Notification of cooperation agreements (Case COMP/C-2/38.377 — BIEM Barcelona Agreements), PbEG 2002/C 132/10, http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/c_132/c_13220020604en00180018.pdf
- BUMA/SABAM (2005): Notice published pursuant to Article 27(4) of Council Regulation (EC) No 1/2003 in Cases COMP/C2/39152 — BUMA and COMP/C2/39151 SABAM (Santiago Agreement — COMP/C2/38126), 17 August 2005,Official Journal C 200, 17/08/2005, pp. 11-12; http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52005XC0817(03):EN:HTML
- Commission staff working document (2005): Study on a community initiative on the cross-border collective management of copyright; http://europa.eu.int/comm/internal_market/copyright/docs/management/study-collectivemgmt_en.pdf
- Contributions to the Study on a community initiative on the cross-border collective management of copyright (2005): http://europa.eu.int/comm/internal_market/copyright/management/management_en.htm
- EDIMA: http://www.europeandigitalmediaassociation.org/
- European Commission (2004): Press Release IP /04/586 of 3 May 2004: Commission opens proceedings into collective licensing of music copyrights for online use ;

http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/586&format=HTML&aged=1&language=EN&guiLanguage=en

- European Commission (2005a): Press Release IP/05/872 of 7 July 2005: Music copyright: Commission proposes reform on Internet licensing; http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/872&format=HTML&aged=0&language=EN&guiLanguage=en
- European Commission (2005b): Press ReleaseIP/05/1056 of 17 August 2005: Competition: Commission consults on BUMA and SABAM's commitments for the licensing of online music; http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/1056&type=HTML&aged=0&language=EN&guiLanguage=en
- Helberger (2004): If you can't beat them, join them – DRM as the future for collecting societies. INDICARE-Interview with André Beemsterboer by Natali Helberger. INDICARE Monitor Vol. 1, No 6/7, December 2004, http://www.indicare.org/tiki-read_article.php?articleId=62
- Santiago agreement (2001): Notification of cooperation agreements (Case COMP/C2/38.126 — BUMA, GEMA, PRS, SACEM), PbEG 2001/C 145/02; http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/c_145/c_14520010517en00020002.pdf

About the author: *Margreet Groenenboom* is project researcher at the Institute for Information Law, University of Amsterdam. She specialises in copyright law, patent law, trademark law and law & information technology. Contact: groenenboom@ivir.nl

Status: first posted 27/09/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=139

Helping libraries manage digital rights

Standards for the electronic communication of licensing terms

By: Brian Green, EDItEUR, London, United Kingdom

Abstract: As the number of digital resources in library collections grows, libraries are reaching out for solutions to help them comply with the differing license terms applied to resources by their creators and publishers. EDItEUR is developing standards for the expression and communication of licensing terms in XML, building on the work of the Digital Libraries Federation's Electronic Resource Management Initiative (ERMI), the joint EDItEUR / NISO work on ONIX for Serials and the analytical approach of the INDECS project. This article summarises the significant progress made towards a solution based on standard message formats and a structured data dictionary.

Keywords: technical analysis – e-journals, libraries, licensing contracts, metadata , publishing, rights expression language, standards

Managing electronic resources

The terms "Digital Rights Management" and "Rights Expression Language" are somewhat unhelpful, often interpreted as having more to do with technical protection and limitation of access than the management and expression of rights. This article, however, addresses the very real issues of how digital rights are to be managed and expressed in an environment of trust – the licensing relationship between academic publishers and libraries.

In this business to business relationship technical protection is neither required nor desirable. The relationship is a contractual one, based on licences and publishers are quite content to trust librarians to comply with the terms of those licences. Libraries may decide to incorporate some degree of technical protection within their own library systems in order to prevent unauthorised use of digital materials, but they do not want to have this imposed by the publishers.

However, as the number of digital resources in library collections grows, libraries are reaching out for ways to help them comply with the differing licensing terms applied to resources by their creators and publishers. Paper licences, once negotiated and exchanged, are duly filed and it becomes a major task to answer a simple question such as "*May I make 20 copies of this article for my class?"* The ability to express usage rights and permissions electronically in a simple form, link to them from digital resources and communicate them to users has become an urgent need. Ideally, an XML message expressing the terms of the publisher/library licence should be generated by the publisher's licensing department and communicated to the library, either directly or through a trusted intermediary, for linking to the relevant resources.

Neither publisher nor library systems have been able to cope with this requirement. One significant obstacle has been the lack of underlying metadata standards necessary for such complex exchanges.

Work on rights metadata standards

EDItEUR (cf. sources) is the international body for e-commerce standards in the book and serials sector, originally set up by the European Bureau of Library and Documentation Associations, the Federation of European Publishers and the European Booksellers Federation. It is now a truly international not-for-profit organisation with members from all of the above communities in USA, Canada, Europe, Asia and Australia developing standards for EDI, bibliographic information and the communication of serials information.

EDItEUR has been working in the area of rights since 1997, when a joint NISO (National Information Standards Organisation; cf. sources) /EDItEUR working party was established to explore the metadata requirements for rights trading. The working party concluded that the essential elements that had to be identified and described were the resource itself, the user and the required use. Progress has been made in the area of resource identification, with the widespread implementation of DOI (Digital Object Identifier; cf. sources) and open URL to identify resources and the development of ONIX (Online Information Exchange; cf. EDItEUR 2005a), and in particular ONIX for Serials, to describe them. The identification and description of users raises privacy as well as administrative issues and, in actuality, the major requirement is not individual identification of users but authentication of their status as a bona fide user. Authentication systems such as Shibboleth (cf. sources) now enable authentication of user status.

There remains the description of usage rights. So-called Rights Expression Languages such as XrML (eXtensible rights Markup Language; cf. sources) and ODRL (Open Digital Rights Language; cf. sources), have been developed primarily for the music and video industries as mark-up languages to drive technical rights enforcement technologies in business to consumer situations. They are, at the same time, both more and less than what is required for the communication of licensing terms information. EDItEUR believed that what was required, and lacking in the rights expression languages, was a highly-structured data dictionary that accommodated the full richness of licensing terms and that could be used to generate messages in various different syntaxes. On the other hand, there was no requirement in this community for messages to directly drive technical protection mechanisms.

This work was picked up in a multi-media context by the EU-funded <indecs> (Interoperability of Data in e-Commerce Systems; cf. sources) project that ran from the end of 1998 to early 2000 and included participation from the various media sectors. <indecs> developed an analysis of the requirements for metadata for e-commerce in intellectual property in the network environment which received widespread support. The work of the <indecs> project has been carried forward in the development of the iDD (indecs Data Dictionary) by the International DOI Foundation (cf. sources) and in the development of the ISO MPEG Rights Data Dictionary - ISO/IEC 21000-6 (cf. Barlas 2005).

The Electronic Resource Management Initiative

Parallel to these developments, the library community was struggling with the wider issues of managing electronic resources and given the inability of integrated library systems to provide comprehensive solutions at the time, individual institutions were developing their own non-interoperable systems. Recognising the shortcomings of such an approach, in mid-2002 the Digital Library Federation launched ERMI (cf. sources), the Electronic Resource Management Initiative to define the functional requirements of an electronic resource management system and begin to develop a common set of specifications which could be followed by the library systems vendors.

ERMI's goals were to:

- Describe architectures needed to manage large collections of licensed e-resources
- Establish lists of elements and definitions
- Write and publish XML Schemas/DTDs (Document Type Definitions)
- Promote best practices and standards for data interchange

These goals were substantially achieved in their final report (Jewell et al. 2004) published in August 2004. Many of the major library systems suppliers have already started building electronic resource management extensions to their systems based on the ERMI reference model.

A number of very complex issues were recognised and modelled, including the complex ways in which licences relate to electronic resources; the need to interpret the lack of a specific statement in licenses (where does such silence imply a permission and where a prohibition); the difficulty of managing the realities of complex user groups and institutional locations.

ONIX for licensing terms

Meanwhile, EDItEUR, had been working in a Joint Working Party with NISO to develop "ONIX for Serials" a family of XML standards to support communication between publishers, agents and librarians primarily as it relates to the management of ejournals.

A requirement for the unambiguous electronic communication of licence terms within this supply chain was identified and EDItEUR commissioned a paper from the Rightscom consultancy (cf. sources) (An assessment of ERMI in the context of ONIX and requirements for recording and communicating licence terms for electronic resources (Bide and Rust 2004), to assess the extent to which the ERMI work in this area might provide a basis for the development of standards for the transmission of licensing terms throughout the supply chain for digital resources.

The assessment paper concluded that the ERMI work was a good starting point for such work but would require further development in order to meet EDItEUR's requirements that a licensing terms message should:

- Take into account the requirements of all stakeholders in the supply chain: libraries, publishers and other rights holders, intermediaries, library users
- Provide for the full complexity of rights expression:
- Be designed to support interoperability
- Be fully extensible in future, to support new business models, all types of use and all media types

The paper recommended the development of a generic ontological structure for rights based on a "contextual", event-based architecture and a well-structured rights data dictionary. This proposal was presented at a seminar on the subject jointly hosted by EDItEUR and NISO in London in December 2004. The feeling of that seminar was that a proof of concept was required to better illustrate the potential of "ONIX for Licensing Terms".

Following the seminar, with funding from the Publishers Licensing Society (PLS; cf. sources) and the JISC (The Joint Information Systems Committee; cf. sources), Rightscom were commissioned to undertake this "proof of concept" project, working with the EDItEUR ONIX technical team (*David Martin* and *Francis Cave*) to explore the possibility of developing an "ONIX for Licences" mes-

sage that could be used by publishers and online hosts to communicate licence terms to libraries and subscription agents (EDItEUR 2005b).

The aim of the project was to produce a prototype XML message for communicating in a computable form the terms of a Licence agreement for the use, by libraries, of a publisher's digital works. The main use case was the licensing of electronic journals, but the structure of the message needed to be flexible enough to be extensible to any other type of digital media and license in future by adding to its semantics but not significantly changing its structure. The message therefore needed to be generic in structure but successfully demonstrate an initial, specialized application.

The prototype message was produced as an XML schema and succeeded in demonstrating that each element of the example licence clauses could be fully modelled. The modelling also highlighted the range of possible variations within even apparently simple licensing clauses, and the limitations of the original ERMI approach that defines only a limited "typical" set of usages with no mechanism for variation. One example of this is the use of the term ILL (Interlibrary Loan), frequently used in library licences.

ILL is not a single permission – it is a complex bundle of permissions, prohibitions and conditions with many variables. These can be expressed in a very generic form – e.g. permits "ILL"; or in a very granular and complex form, e.g.

> *permits a librarian at institution "A" to make a copy of a defined part of resource "X" in physical (but not digital) form and sending that copy of part of resource "X" to a librarian at another institution "B" – subject to the condition that institution "B" is in the same country as institution "A" – and then the librarian at institution "B" may pass that copy of part of resource "X" to a user – subject to the condition that the user is an employee of institution "B" and is using the copy for academic non-commercial research – and all subject to a condition that the librarian at institution B maintains a record that the copy was made.*

The ONIX for Licensing Terms message needs to be able to handle either the generalised term or the complex form.

Further development work has been carried out and a draft format of the ONIX for Licensing Terms message with examples is now available on the EDItEUR website http://www.editeur.org. ONIX for Licensing Terms requires that a formal definition is provided for:

- (a) Each "party" that is mentioned anywhere in the license.
- (b) Each "resource" that is mentioned anywhere in the license (including resources that are derived by actions taken under the license, eg extracts made from the original licensed materials).
- (c) Each "time" or "place" that is mentioned anywhere in the license.
- (d) Each external "document" (paper or electronic) that is referenced anywhere in the license.
- (e) Each "usage" that is referenced anywhere in the license.

In each definition, a "label" is assigned that must be unique within the License Terms document, and this label is used elsewhere in the XML to refer to the entity that has been defined.

The definitions are crucial to the ONIX Licensing Terms structure, and are likely to be the largest section of a License Terms XML document.

The key elements in the ONIX Publisher Licensing Terms format carry controlled values which will be managed through a structured dictionary – the ONIX Licensing Terms Dictionary.

Next steps

However, in addition to the technical work remaining, there are still several practical and political issues to be dealt with:

- Publishers, especially small and medium sized ones, will need tools and services to help them produce the XML representations of their licences

- Integrated library systems will need to implement the standards in the electronic resource management systems that they are developing.
- Some librarians are concerned that the development of licensing messages represents "the thin end of the wedge" in terms of introducing DRM enforcement technology into the relationship among publishers, libraries and library users. (In fact, the fuller compliance to licensing terms that this work will facilitate makes the implementation of technical protection measures even less likely or attractive to publishers).
- There are concerns that the precision required to automate the exchange of licences could remove deliberate ambiguity in a licence that is sometimes key to the successful conclusion of negotiations.
- There are issues about whether the paper or the electronic version will be the canonical licence (and where liability lies if a system misinterprets a licence term).

A new Joint Working Party of ERMI, EDItEUR, NISO and PLS is now being set up to carry the work forward, further develop, pilot and promote the messages. The organisations forming the new joint working party and representing libraries, publishers and standards bodies are optimistic that by pooling resources and working collaboratively, these issues can be sensibly discussed and dealt with. Any readers interested in learning more or becoming involved in piloting the messages are invited to contact the author.

Sources

- Barlas, Chris (2005): Introduction to ISO/IEC 21000-6 Rights Data Dictionary: ISO/IEC JTC 1/SC 29/WG 11/: http://www.chiariglione.org/mpeg/technologies/mp21-rdd/
- Bide, Mark; Rust, Godfrey (2004): An assessment of ERMI in the context of ONIX and requirements for recording and communicating licence terms for electronic resources: EDItEUR
- DOI and Data Dictionaries: DOI factsheet: http://www.doi.org/factsheets/DOIDataDictionaries.html
- EDItEUR: http://www.editeur.org
- EDItEUR (2005a) ONIX Publisher Licensing Terms draft format: http://www.editeur.org/onix_licensing.html
- EDItEUR (2005b): Licensing Terms: report on a "proof of concept" project commissioned by EDItEUR from Rightscom and jointly funded by the Publishers Licensing Society (PLS) and the Joint Information Systems Committee (JISC): http://www.editeur.org/licensing/OLT_proofofconceptreport.pdf
- ERMI: Digital Library Federation Electronic Resource Management Initiative: http://www.diglib.org/standards/dlf-erm02.htm
- <indecs> project: http://www.indecs.org/
- Jewell, Timothy; Anderson, Ivy: Chandler, Adam; Farb, Sharon; Parker, Kimberley; Riggio, Angela; Robertson, Nathan (2004): Electronic Resource Management: the report of the DLF initiative, Digital Library Federation: http://www.diglib.org/pubs/dlfermi0408/dlfermi0408.htm
- JISC: http://www.jisc.ac.uk/
- NISO: http://www.niso.org/
- ODRL (Open Digital Rights Language): http://odrl.net/
- Publishers Licensing Society: http://www.pls.org.uk/ngen_public/default.asp
- Rightscom: http://www.rightscom.com/
- Shibboleth project: http://shibboleth.internet2.edu/
- XrML (eXtensible rights Markup Language): http://www.xrml.org

About the author: *Brian Green* is Manager of Book Industry Communications, the UK book and serial industry standards body set up in 1991 by The Publishers Association, The Booksellers Association, The Library Association (now CILIP) and The British Library. He also manages EDItEUR, the international umbrella body for book and serials standards. Brian is active on many international standards committees and chairs ISO TC46 SC9, the ISO subcommittee concerned with identifiers and metadata. Brian can be contacted at brian@bic.org.uk

Status: first posted 28/09/05; licensed under Creative Commons
URL: http://www.indicare.org/tiki-read_article.php?articleId=140

Business models and rights management for eLearning in Europe – Findings of the OrmeE project

By: Paola Mazzucchi, AIE – Associazione Italiana Editor, Milan, Italy

Abstract: The purpose of this article is to highlight the key findings of the OrmeE Project (Observatory on Rights Management for eLearning in Europe). First the general context is presented, then the relevant legal framework is introduced, and thirdly 9 different business models for educational e-content markets are sketched.

Keywords: project description – business models, copyright law, e-learning media markets, EUCD, publishing, education – EU

Introduction

Education in the digital age is a much more complex issue than one could imagine. It is easy to pronounce words as e-schools, e-classes and e-learning. They sound fashionable and trendy but what do they actually mean? Education in the digital age means that teachers can use new technologies to teach and learners can use new technologies to learn. But the real question is: what do they teach and learn? Is the educational environment ready to shift from old and good paper schoolbooks to digital content? How does the value chain of educational content need to be reshaped in order to create a sustainable market for all key actors: publishers, teachers and learners? And which role do public institutions on both the national and European level play?

The purpose of this article is to highlight the key findings of the OrmeE Project (Observatory on Rights Management for eLearning in Europe; cf. sources) with respect to the management of copyright related to educational content in the digital environment.

Talking about copyright for digital educational content requires, however, a preliminary description of its context. The basic question therefore is: *Why is digital rights management a relevant topic for the educational environment?* One question, three answers:

First, in the last 5-10 years all European school systems have been deeply affected by the need to introduce information and communication technologies (ICT) in schools. This process has also been driven by EU policy objectives according to the Lisbon strategy: to achieve a harmonized and standard level of "digitalisation" in all economic and social areas (i.e. e-government, e-health, e-learning, e-business, e-inclusion) and to diminish the digital divide between the Us and the European Union.

Second, EU legislation on copyright – in particular on digital copyright – to be implemented at the national level aims to establish a common framework for all Member States in order to further the uptake of the European and global digital content markets and at to maintain at the same time some exceptions for educational purposes.

Third, even without taking into account the previous considerations, a market for digital educational content is actually emerging at it is growing at European level. Its development will probably follow the path drawn by the US.

The legal framework of copyright in the digital era

The penetration of digital technologies (in households, public institutions, offices and companies) means a rapidly growing number of people who can have access to digital information and knowledge. This enables the growth of a market for digital content, both for existing content and new added value services. This evolution process has already led to new problems related to copyright protection. Today digital technology allows perfect and unlimited copying and distribution of content in a quite inexpensive way, and this is true for copyrighted digital content too. As a consequence, the European

legislator introduced new regulations concerning protection and enforcement of intellectual property rights with a major role for DRM systems, in particular: Directive 2001/29 (cf. sources) and 2004/48/EC (Enforcement of Intellectual Property Rights; cf. sources).

Directive 2001/29 establishes a framework which balances incentives to create and distribute content –serving the interest of the public (and individual users) – with mechanisms ensuring appropriate revenue through the exercise of intellectual property rights.

"Copyright and related rights play an important role in this context as they protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content". (Directive 2001/29, Art. 2)

The need for a common system (and a common basis) to regulate the market, to protect copyright and to grant rightholders a fair compensation, is much more urgent, because the existence of such a market for digital content depends on the existence of a "standard" regulation. Only if these conditions will be met, it will be possible to develop economically sustainable business models for the "commercialisation" of digital content. From the OrmeE perspective, this issue is even more significant as the Directive itself allows for exceptions concerning the educational environment.

Despite the stated goal of harmonising national copyright legislations, the implementation of the 2001 Directive has not yet achieved much in making the exceptions in the field of educational uses converge. Member States have made use of the possibility provided for by the Directive to implement several exceptions differently. Some have implemented the text of the Directive literally, others simply kept their national provisions considering them in line with the Directive, other Member states have not yet implemented the Directive, and others deliberately used the freedom of decision left to them by the Directive.

As a consequence what is to be understood as "use for the purpose of illustration for teaching or scientific research" will continue to differ from country to country in different respects. In particular we will have to deal with national copyright legislations that:

- don't include an exception in relation to educational and scientific use,
- do include such an exception in the broadest meaning possible (i.e. in conformity with article 5.3.a Copyright Directive), or
- do include such an exception but with a narrower scope of application.

Differences can be identified with respect to the following questions:

- Which acts may be performed (reproduction and/or communication to the public)?
- What may be used (all works or only certain literary works)? How much may be copied (only excerpts of materials or the entirety)?
- What is meant by the "for the sole purpose of illustration for teaching or scientific research"? Where is the limit? Has a remuneration to be paid to compensate for the free use?

As long as national laws differ – and it is extremely difficult to foresee whether this will ever change especially now that the Union counts 25 Member States -, specific acts related to education and teaching may be allowed by the law in one country but forbidden in another country. It is therefore crucial to find and support *best practices* that demonstrate the actual possibility to combine copyright protection and effective access to content by educational organisations and individual learners.

DRM and education

Over the past few years, the world of textbook and educational material publishing has been marked by the advent of digital technologies. The ongoing process of innovation and media integration has led to a complete change in the culture industry.

As a result, a new digital educational content market is emerging with a new commercial approach (as has already happened in other

areas of publishing, such as legal databases and university publishing): from the distribution and sale of tangible products to the distribution and licensing of intangible products, and from products to the services.

In this new context, the textbook publishers, who once based their activities on the production of textbooks and by this maintained their undisputed leadership in the educational content market, must now seriously reconsider their role. They have to find a way to deal with their new competitors, which include companies specialised in e-Learning or technology companies. These have been uninterested so far in the production of educational material, but now – based on their skills and competencies – they consider the world of educational publishing as a lucrative new business..

Copyright management becomes essential in this scenario – in technical and economic terms as well - of an educational content market that can only be conceived in a transnational form, given the enormous potential offered by digital technologies, and in particular, by the primary vehicle for digital content: the Internet. In light of these factors, DRM becomes a topic of discussion – and an urgent need - for the entire educational sector.

DRM and the educational publishing industry

In fact, it has already been mentioned that the application of DRM solutions is relevant to the creation of a single market for digital educational material. In this market the players have to make strategic choices as regards the licensing models to be adopted. This requires previous assessment of the sustainability and consistency of available options in the context of national and European regulations. Viable business models have to meet both, the needs of the educational world and the need of economical sustainability for the actors involved, whether they be content providers, aggregators, or distributing intermediaries.

As far as business models are concerned, it is hard to define one best solution, as the players involved and their relationships vary from case to case depending on the target markets and their specific products or services. It is also worth mention that the adoption of complex DRM systems by educational publishing houses is far from being fully developed. On the contrary: they tend to use hybrid solutions, managing certain aspects of the described digital content value chain without setting up an integrated system.

In the following we will examine different business models in order to highlight underlying trends and perspectives.

Model 1: Textbook publisher delivers his own content through his own web site or dedicated portal

This is one of the easiest business models to describe, as there are few players involved: the publisher as rightsholder and the end user. From the DRM point of view this means that the publisher end-user relation is regulated by the license agreements between the two parties. The choice to exploit in-house resources and know-how and to deliver this digital educational content via the publisher's web site or portal is very common among traditional textbook publishers.

In this case all decisions concerning the adopted business model depend on just one single player: the publisher. Once this business model is successful, it is likely that the same content will be delivered according to further business models, e.g. contributing to a delivery system launched by a public aggregator (e.g. Ministry of Education).

Model 2: Textbook publisher delivers his own content through an e-learning platform developed in house

Maintaining a learning platform implies that the digital content delivered (learning objects) should comply with the most common international standards. In general platforms are standardized (mostly Scorm compliant; cf. sources). It would not be wise to develop an in-house learning platform with proprietary formats because the publishers would not be able to deliver the same content in other ways, e.g. by means of an aggregator.

Like in the model described before, the educational publisher is the main player. It goes without saying that an educational publisher must also have strong ICT know-how in ad-

dition to editorial and content production skills. This is usually the case when an e-leaning provider is a spin-off of an educational publisher.

Model 3: Private aggregator gathers and delivers third party content

Private aggregators operating in the digital educational environment collect resources not only from educational publishers but usually also from other content providers such as newspapers, TV broadcasters or e-learning content developers – thus granting the user access to a very complex and articulated product.

Educational publishers should be the main content providers because they have the necessary skills, experience and knowledge for the production of educational content. Reliance on an aggregator could also be a good opportunity for small and medium sized publishing houses that cannot afford to enter the digital market by developing their own in-house delivery system.

Model 4: Public aggregator gathers and delivers third party contents

Aggregators of educational content are often private companies supported by a public institution (such as the National Ministry of Education). This institution is usually financing and launching a project for schools granting access to digital educational resources. Often they also finance the purchase of the content delivered on-line.

Educational publishers should play a prominent role in content provision, even though it sometimes seems that public aggregators tend to develop their own educational content (e.g. commissioning resources to pools of experts), thus keeping educational publishers in a marginal position.

It should also be understood to what extent participation in a public aggregator service is linked to some kind of quality certification of the digital material and who is in charge of approving or rejecting the content. This type of selection is usually closely linked to the system of selection and approval of textbooks in each country's education system. We might therefore imagine a "quality assessment" for educational digital content that regards only the structure of the content (e.g. compliance with international standards, metadata, level of interactivity required) and not the control of the content itself.

Model 5: Gateway

A gateway could be defined as a bibliographic database for digital (but also print) content. This could be a metadata repository of content. Usually gateways of educational resources are "sponsored" by public institutions, mostly in those countries where schools receive funding to purchase electronic resources.

Relying on a gateway for an educational publisher means having a wider visibility and reaching a broader audience. This model presumes of course that the educational publisher has defined his own business model and set up his own delivery system.

Model 6: Textbook publisher provides schools with a bundle of content

This rather uncommon business model implies that a single content provider, such as an educational publisher has at his disposal highly developed interactive content, infrastructures and ICT skills to offer an all inclusive solution to schools. Obviously, the business model can be sustainable only for large size educational publishers, usually as part of a corporate group with assets in other content industries.

Model 7: Content aggregator provides schools with a bundle of content

In general, this solution closely resembles an all-inclusive offer to schools where content produced by different content providers has been structured and "packaged" in order to create consistent lessons. This means that licensing to the end user is totally up to the aggregator which actually sells a product, while educational publishers have to manage economic contracts with the aggregator itself.

Model 8: E-learning environment offers services and gathers educational content

It is rather difficult to classify this kind of business model because there are many different stakeholders along the value chain. Content could be developed and implemented either directly by users or user communities, or by commercial content providers

(educational publishers or e-learning content providers), or by pools of experts involved in the project.

This is a very interesting business model as schools, teachers and students are directly involved in the process of content creation and knowledge growth. Therefore they feel more engaged. It is however still not clear how the relationship (even economic) between the parties shall be regulated.

Model 9: E-learning content e-platform provider develops a courseware solution

If, as described in the previous business models, educational publishers tend to play a significant role in the content creation process, this last solution is totally up to players traditionally outside the educational/ publishing market. Here the main player is a technology provider specializing in e-learning, developing the technical platform as well as the content (learning object).

Which role might educational publishers play in here? Apart from being targeted clients themselves, they might be able to act as partners for the development of reliable contents.

Bottom line

OrmeE – (Observatory on Rights Management for eLearning in Europe) is an innovative project financed by the European Commission in the framework of the eLearning programme. The project partners are: AIE (Italian Publishers Association), FEP (Federation of European Publishers, TUB (Technische Univeristät Berlin) and Bologna Fiere (Organizer of the Bologna Children's Bookfair). In other words, OrmeE is strongly driven by the publishing industry perspective, aiming at defining the role educational publishers could (or should) play in the competitive arena of the growing market of digital content.

Sources

- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf
- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights; online available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf
- SCORM (Sharable Object Content Reference Model) at the Advanced Distributed Learning web site: http://www.adlnet.org/scorm/index.cfm
- The OrmeE website is available at: http://www.ormee.net

About the author: *Paola Mazzucchi*, AIE – Associazione Italiana Editor, is member of the OrmeE team and will take all your questions related to this article, and will, if necessary, forward them to the experts involved in the project. Contact details: info@ormee.net

Status: first posted 29/09/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=142

Digital rights in the information society – opportunities and challenges regarding citizens' access to information

By: Jacob Skjødt Nielsen, the Danish Board of Technology, Copenhagen, Denmark

Abstract: The Danish Board of Technology is issuing a report on the consequences and implications of digitalisation and DRM. The report gives recommendations regarding the use of DRM within the public sphere. Aiming to balance between consumer interests and content owners' legitimate rights, a working group of stakeholders has been set up trying to identify and agree on challenges and opportunities for public information providers. Differences in the assessment of DRM technologies and lack of practical experience, however, proved an almost insurmountable obstacle.

Keywords: policy analysis – copyright law, consumer expectations, consumer rights, EUCD, interoperability, libraries, stakeholders – Denmark

Aiming for balance

A working group set up by The Danish Board of Technology is about to issue a report on the project "Digital rights in the information society" (Teknologirådet 2005). Over the past year the board has facilitated a stakeholder discussion of the consequences and implications of the digitalisation of information and DRM. The aim is to provide politicians and decision makers with an overview of the discussion, and to provide recommendations regarding the use of DRM within the public sphere. The main objective and at the same time the key challenge was to strike a balance between consumer interests and content creators' legitimate rights. It would be a Pyrrhic victory indeed should the digital technologies, promising new possibilities for communication and distribution of information, instead lead to restrictions, limitations and boundaries for citizens' access to digitalized information. It is therefore evident that a balance must be restored between consumer interests and content creators' legitimate rights.

DRM – the problem solved?

The report describes how the term Digital Rights Management (DRM) has been used to describe dissimilar technologies (Dykstra 2003). Since DRM, as of today, is not considered a clearly defined concept, stakeholders have produced equally diverse assessments. This in turn has led to much discussion in the group about the usefulness of such a concept. Moreover, practical experiences are limited in relation to the implications as well as the benefits of this technology (or technologies). Some stakeholders expressed great expectations regarding the future potential of DRM technology, while others expressed equally strong technical reservations and privacy concerns. Evidently, insufficient experience with the practical application of DRM systems and uncertainty about their technological potential has made any assessment dubious.

The most important arguments *for* DRM are that DRM can increase protection against piracy and illegal distribution of content and make technical enforcement of rights possible. Furthermore, using DRM new business models and distribution forms can be established for instance through direct distribution to the end consumer.

The most important arguments *against* DRM are that DRM can technically hinder the moving of information between platforms and applications - which in turn will undermine interoperability and the opportunity for the user to choose technology. Furthermore, legal protection of DRM can reduce innovation and research in digital technologies and thus the competition on this market. Finally legal protection of DRM can erode exemptions for certain user groups provided by the Danish law on copyrights / intellectual property right.

Among the participants of the working group, there were different interpretations of the consequences the implementation of the

EU InfoSoc directive (EUCD 2001) might have in this respect. Some said the use of DRM technology as defined in the directive would *de facto* prevent the use of certain consumer exemptions granted by the law, while others held that it was a minor issue with limited practical consequences and, furthermore, that the rightholders should be conceded the privilege to limit or expand consumer access.

The case of netmusic

Facing these opposing assessments the members of the working group chose to work with an exemplary case, i.e. public libraries including research libraries. Libraries seemed an obvious choice since they provide access to a broad range of information that is increasingly available in digital formats, while they are also obligated by law to provide free access for their national audiences as well as to ensure quality, diversity and actuality (Thorhauge 2005). The case included past experiences and future expectations and challenges libraries are facing with respect to digital information.

One of the key elements was the concept of "netmusic", a service hosted by the public libraries that allows citizens to download music over the Internet and listen to it in a period of seven days free of charge (see also Nielsen 2004). Netmusic is based on Microsoft's DRM system, which as of now means that music playback is limited to the Windows Media Player, thus excluding users of Linux, Mac, portable music players and home stereo devices among others. The explanation for this choice of DRM is that only this particular brand could reassure content providers on safety issues and make possible an agreement on the terms. The consumer is thereby licensed to listen to, but not copy the music. Today the netmusic service includes around 6,500 albums. Some 800 tracks are downloaded daily, which comes to a modest 0.2 percent of the total loan of CDs. The service is being criticised for lack of variety as well as disregard for most consumers' music listening behaviour (Teknologirådet 2005).

It is still only a relatively small selection of digital works that are available at the libraries, when it comes to books, music and films, while research articles are widely digitalised. The former is in part due to lacking or insufficient agreements between libraries and owners of rights, while the latter is due to the relatively limited risk of mass distribution. Furthermore most agreements on distribution of research journals and articles are negotiated at international level.

Since the working group consisted of several stakeholders, the discussions and disagreements on DRM reflected many of the conflicts that one may find in the more general debate on the relation between private and public information providers. To some, DRM represented a possible basis for new agreements and business models, while also preventing piracy. To others, DRM systems constituted a technical system that could take precedence over the legal system and shift the balance between consumer rights and the holders of rights. So it seems that the technical discrepancies of the assessment of DRM were repeated on an institutional level.

An important conclusion from this work therefore is that it is impossible to assess technology as such – without considering the possibly conflicting perspectives that different stakeholders may have on the use of such technology. In technology assessment (TA) this insight is far from new – but it is often forgotten.

Striking a balance?

The two main problems

Using public libraries as an example, the work group has considered the conditions for the implementation of DRM technology. Without reaching an agreement, however, it was debated whether the legal protection of technical protection measures (TPM) might actually put citizens and public providers of information at a disadvantage when using digital works as compared to analogue works. When the EU InfoSoc directive was implemented in Danish law, it was decided to maintain the exemptions stipulated in Chapter 2 of the Danish Copyright Law, but it has remained a disputed question, whether the use of DRM will render some of these exemptions impractical (Teknologirådet 2005).

According to some, users must be able to freely decide what to download and when, in order to ensure that the potential of digital technologies is fully utilized. Whether this is possible without affecting the conventional use of the material or violating the legitimate interests of the copyright owners, however, was not agreed upon.

The work group has not taken into consideration which division of tasks between public and private providers of information would be most appropriate in the future. Should public providers of information continue to play a mayor role in the general supply of information?

Two main problems will arise in any case: the need for new usage rights and the need to develop new DRM systems which meet new requirements.

1. New usage rights

In order to make better use of new technologies, it is imperative that copyright owners and public providers of information agree on new usage rights in relation to the distribution and consumption of digital works. Such agreements between the parties have proven difficult to achieve due to the copyright owners' general hesitation to make digitalized information available for public distribution and usage. The main reason for this is the risk of illegitimate use and distribution of content. Should such agreements result in an increased uncompensated use of copyright holders' works, this may necessitate increased financial funding. Also it may become necessary to establish other clearing agreements. If new usage rights are not established, this may lead to a decrease in the volume of digital works accessible to the public. Likewise, the available volume of works may not be able to meet the demand in terms of quality, diversity and actuality.

2. Required features of DRM Systems

Danish politicians and officials should try to reach an agreement on the required features of DRM systems, and they should consider to work towards an international standardization of DRM systems. The alternative may be a proprietary market that may be harmful for competition and put users at a disadvantage.

Clearly, public stakeholders – potentially large users and consumers of DRM – should demand special features of these systems and thus ensure certain minimum standards, such as interoperability and open standards. As described earlier, the various types of DRM technologies differ greatly. It is therefore highly important to assess how much particular systems may interfere with the behaviour of consumers. The question remains, however, if systems that merely state the relevant copyrights to the end-user would suffice, or if we should implement systems that serve to further regulate user behaviour, such as the system already employed by Danish public libraries in their digital music service "netmusic" or even Trusted Computing. The disadvantages of the latter are the potential limitations of free choice of technical platforms and privacy concerns (Schneier 2005). Politicians ought to debate whether DRM technologies used within the public domain must take into account the consumer exemptions stipulated in Chapter 2 of the Danish Copyright Law.

The need for further debate and coordination

Inherent in this discussion on the consequences and implications of DRM and digital distribution by public providers of information, are problems and challenges related to a range of different political domains.

Legal problems and challenges

- Do DRM systems and their ability to enforce conditions of use across national borders, including the collection of personal data, make it necessary to change the existing laws?
- Furthermore, should the present legal protection of DRM technology in the Danish Copyright Law be continually reviewed?

The Danish Parliament should take this into consideration when reviewing the rules of the legal protection of technical protection measures of the Copyright Law.

Market related problems and challenges

- Should we establish new usage rights that make it possible for public services to distribute digital works?

- Do we need to keep an eye on the level of competition involved in the use of DRM technology?
- Is there a risk that the legal protection of DRM can serve to keep unwanted competitors off the market?

Technological problems and challenges
In order to enhance free competition the various DRM systems should be interoperable and it should be secured that using DRM technology will not violate citizens' rights of privacy.

- Which features should public providers of culture and information then require of DRM systems?
- Should the various public stakeholders be able to make individual DRM-agreements with copyright holders, or should the public as such require a set of general features?

Problems and challenges of cultural policy
Publicly financed cultural institutions must continually secure a selection of digital works that adheres to the legally binding demand for quality, diversity and actuality.

- Which features must they then require of DRM systems and the production of digital content in order to be able to fulfil these obligations to the public – just as they have hitherto been able to fulfil the legally binding obligations in reference to analogue material?
- Is it feasible that new usage rights can be established on the basis of the present financial resources – or is further funding necessary?

Bottom line

In conclusion, the experiences are limited and DRM is still a technology in the making. Public libraries and other information providers have yet to explore the possibilities of both digitalised information and DRM, with respect to their obligation to meet certain standards of quality, diversity and actuality. Therefore the parties need to form agreements on the right of usage of digitalised information. As a part of this agreement DRM technology should be considered, but to ensure interoperability an open standard may be required.

To fully explore these findings the Danish ministries of Culture, of Science, Technology and Innovation and of Economics and Business Affairs should intensify their corporation in the areas mentioned. Furthermore, politicians and officials should continue the attempt to establish a wider consensus on the long-term prospects in order to attain a balance between the copyright holders' legitimate demand for payment and the citizens' need for free access to information.

Sources

- Dykstra, Gail; Rosenblatt, Bill (2003): Integrating Content Management with DRM: Imperatives and Opportunities for Digital Content Lifecycles: DRM watch: http://www.drmwatch.com/resources/whitepapers/article.php/3112011
- EUCD: InfoSoc-directive in Danish (2001): http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=da&numdoc=301L0029
- Henten, Anders; Schneider, Markus (2005): DRMS and TCP - Technology and Law: Center for Tele-Information: http;//www.cti.dtu.dk/publications
- High Level Group on Digital Rights Management (2004), Final Report: http://europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/doc/040709_hlg_drm_2nd_meeting_final_report.pdf
- Netmusik website: http://www.bibliotekernesnetmusik.dk
- Nielsen, Kurt Westh (2004): Net music the Danish way: Locked down and easily cracked: INDICARE: http://www.indicare.org/tiki-read_article.php?articleId=55
- Schneier, Bruce (2005): Is Microsoft skirting the issue?: ZDNet: http://news.zdnet.com/2100-1009_22-5844520.html
- Teknologirådet (2005): Digitale rettigheder i informationssamfundet – muligheder og udfordringer for borgernes adgang til information: http://www.tekno.dk/drm
- The Danish Board of Technology: http://www.tekno.dk

► Thorhauge, Jens (2005) “Public Libraries in the Knowledge society, Paper from III Public library Conference in Topusko, Croatia: http://www.bs.dk/default.aspx?lang=en

About the author: *Jacob Skjødt Nielsen* is a project assistant at the Danish Board of Technology and a Master’s student of social science and technology. Contact details: Jacob Skjødt Nielsen, phone direct +45 33455361, e-mail jsn@tekno.dk, The Danish Board of Technology, Antonigade 4, DK-1106 Copenhagen K, Denmark, www.tekno.dk

Status: first posted 29/09/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=143

Editorial of INDICARE Monitor Vol. 2, No 8, 28 October 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: Two articles in the present issue of the INDICARE Monitor challenge the techno-legal content protection paradigm in different ways; a) by pointing to business models exploiting either side effects of piracy or leveraging degradation of (illegal) content; and b) by demonstrating – for a niche segment of the online music market – that a business model based on reciprocity can lead to voluntary payments. In addition you will find a cautious investigation of the question if and how Creative Commons can take advantage of TPMs, and a careful analysis of a law suit dealing with Apple's protectionist FairPlay strategy from the perspective of competition law. Finally we present a very selective review of four recent OECD studies on segments of the digital media industry – filtering out what the OECD has to say about DRM.

Keywords: editorial – INDICARE

About this issue

Alternatives to the techno-legal content protection paradigm

Vural Ünlü, consultant and author of a book on "Content Protection – Economic analysis and techno-legal implementation" starts from the assumption that loss of revenues in the music industry is indeed to a significant extent due to copyright infringements. Based on sound knowledge of network economics he argues that there are business models to fight piracy and to regain revenues without strong technical protection measures (TPM). Responding to consumer needs by increasing the utility of products and services is key. Two strategies are discussed: one in which side effects of piracy are exploited, and a second in which content degradation is suggested, i.e. ways to increase the utility difference between original and pirated products by either combining media products with services difficult to copy, by increasing transaction costs for illegal offerings, or psychological devaluation of pirated goods.

While Ünlü provides theoretical background why increasing utility makes DRM protection less necessary, *Tobias Regner* and *Javier Barria*, both researchers at Imperial College London, have investigated a case in point: Magnatune - an online music label with ca. 200 artists on contract and at the same time an online music shop. What makes it specific is first that the online store allows unlimited streaming or, in other words, informed choice before purchasing, and second that buyers can choose the price they are willing to pay within a range from US $ 5 to 18. The researchers performed an empirical analysis based on data provided by Magnatune and found among other things that buyers pay considerably more on average than the minimum of US $ 5. They conclude that this consumer behaviour is due to the consumer friendliness of the service, encouraging people to reciprocate and thus to pay more than required. They admit that this finding refers to a niche market and "cannot be easily applied to the mass market".

CC and TPM

Jordan S. Hatcher has worked at the AHRC Research Centre at the University of Edinburgh on a study exploring the possibility to use Creative Commons licenses for public sector information. One of the research questions he investigated was if CC licenses are compatible with technical protection measures. For the INDICARE Monitor he expands on this subject very cautiously. First he investigates password protected authenticated environments (e.g. intranets, virtual learning environments, digital repositories) and concludes that CC licenses do allow password schemes. Second, he analyses TPMs attached to actual works in order to guarantee integrity, tracking of use, and prevention of commercial use. He concludes that cautiously applied TPMs "can be used to enhance the attractiveness of CC licenses". What is also worth highlighting is that public sector organizations obviously have different needs than individual authors - a perspective

that is often not taken into account in discussions on CC.

FairPlay plays fair from the point of view of French competition law

Natali Helberger thoroughly discusses an interesting law suit in which a French media company whose activities include running online music stores wanted to get access to Apple's FairPlay DRM system in order to be able to offer its music in a format suitable for the iPod. The question was if Apple could be forced on the grounds of competition law to license its technology to a media company interested in increasing its customer base. The legal concept called "Essential Facilities Doctrine" was the legal lever used to open access to Apple's DRM system. It did not work out for the media company. This article, apart from being an interesting piece of legal reasoning, can also be read as a chapter in the standards war. For INDICARE of course the consequences of these strategies and battles for consumers are of utmost interest and consequently addressed in Natali's contribution.

Review of OECD studies

The Working Party on the Information Economy (WPIE) of the OECD has published four reports on digital media dealing with scientific publishing, music, online computer games and mobile content. The studies aim to describe these sectors in terms of changing market structures, business models, value chains etc. DRM is not a central issue in these studies. Nevertheless we wanted to find out what stance the OECD takes in these matters. *Philipp Bohn* has taken a closer look and discusses what the OECD has to say about DRM. In the field of scientific publishing, especial Open Access publishing, the OECD does no see a role for DRMS. In music markets DRMS may play an important role protecting intellectual property rights. With respect to mobile music policy issues related to DRM are highlighted (e.g. infrastructure, interoperability). In the study on computer games DRM has not been an issue – although it is mentioned once. The OECD admits that further studies into DRM may be required, and in fact, meanwhile another division of the OECD, the OECD CCP Secretariat of which the European Commission is an active member – CCP meaning Consumer Policy Committee – has prepared an issue paper on DRM, which however is not yet publicly available – but watch the following space: http://www.oecd.org/department/0,2688,en_2649_34267_1_1_1_1_1,00.html.

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 28/10/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=151

Profitable piracy and content degradation

An alternative to strong content protection

By: Vural Ünlü, Cogitans Consulting GmbH, Munich, Germany

Abstract: In the quest to safeguard their means of existence, the media industries have been focusing on techno-legal content protection in an isolated and excessive manner and neglecting consumer interests in their profitability calculus. Economic reasoning shows, however, that the reflection of consumer needs in the design of DRMS is of pivotal importance. Selfish economic reasoning demonstrates that decision makers in the media industry must analyse and integrate the notion of consumer utility in their overall strategy. The paradox of profitable piracy and content degradation strategies are discussed that must be taken into account when deciding on an appropriate level of copyright protection.

Keywords: economic analysis – business models, consumer expectations, DRMS, economic theory, media markets, piracy

Introduction

Media managers are complaining heavily about piracy. Although the scale of losses claimed by their representative bodies should be accepted with caution, it can still be seen that the dimension of content piracy is substantial. The significant decrease in revenue cannot be explained in terms of ageing demographics, the excess revenues generated during the vinyl-to-CD conversion cycle and greater competition for the disposable income of young consumers, but rather is to a significant extent attributable to copyright infringements (C.S.a.T.B. 2000).

The techno-legal paradigm of strong protection

In a situation with extensive intellectual property piracy, where current legislation fails to provide the necessary security, media companies are developing self-help mechanisms in order to safeguard sustained sources of direct revenue. The content industry is determined to address this critical situation by seeking techno-legal means of preventing the uncontrolled redistribution of content. *Technical strategies* aim to protect the economic interests of media companies through the deployment of Technical Protection Measures based on key technologies such as encryption, watermarking and rights expression languages (Ünlü and Hess 2004). In this context, Charles Clark has stated that "The answer to the machine is in the machine" (Clark 1996); in other words, the survival of the media industries presupposes the development of suitable technical infrastructure. Technical strategies are effective only when accompanied by contract-based *legal strategies* (e.g. mass market licenses or technology licenses) and by an appropriate legal framework that supports the use of DRMS solutions by ensuring the protection of technical measures (Bechtold 2002). In fact, the technological and legal approaches provide mutual support for one another, thereby constituting a protective unity. Technology prevents infringements, while legal measures provide deterrents regarding circumvention of the technology.

In the quest to safeguard their means of existence, the media industries have been focusing on techno-legal content protection in an isolated and excessive manner and neglecting consumer interests in their profitability calculus. Numerous voices support the so called "Napsterization" threat model that assumes that one crack is sufficient to enable a pirate to inject the content into P2P networks, leading to the perfect public good problem, a phenomenon also referred to as "ROCE" (Rip Once, Copy Everywhere). Therefore, in accordance with the Napsterization model, the DRMS security design selected must be absolutely bullet-proof in order to prevent a single attack which threatens the entire economic value of the content.

A paradigm based on consumer needs

However, this would not make sense, either from a technical or from an economic per-

spective. From a technical viewpoint, it will never be possible to implement complete protection. Even if technological protection measures can remain a step ahead of the attack techniques and tools of the hacker community, the fundamental problem of the "analogue hole will continue to exist. This refers to the possibility of digitising high-quality analogue copies and distributing at least one copy in media networks, with the resulting snowball effects (due to the problem of the "digital hole). Thus, sooner or later, the availability of unauthorised copies must be expected.

In economic terms it is not necessary to increase protection levels excessively or to make technical installations bullet-proof. DRM systems have a substantial price attached to them. The costs of setting up, deploying and maintaining the technical infrastructure seriously erode revenue potentials (Ünlü and Hess 2005). Therefore, in some situations weaker protection may be preferable to stronger forms of content protection. Shapiro and Varian summarise this by stating, "The important thing is to maximise the value of your intellectual property, not to protect it for the sake of protection" (Shapiro and Varian 1999). The need to fine-tune the level of content protection is a well-investigated research issue. Empirical case studies show that liberal download sites with a low protection level, such as iTunes, have proven successful in the marketplace, while many strong content protection systems, such as Sony´s Key2Audio system, have been outright commercial flops (von Walter and Hess 2004).

Thus, economic reasoning shows that the reflection of consumer needs in the design of DRMS is of pivotal importance. Therefore, this contribution seeks to show that decision makers in the media industry must analyse and integrate the notion of consumer utility in their overall strategy. The technical design of DRMS and the scope of content protection must be aligned to consumer interest and the given competitive situation. For this purpose, more abstract industrial organization-models are helpful to determine this optimal level of protection and understand how this level depends on the given market structure (Yoon 2001).

The following arguments demonstrate that a lower level of technical content protection can both satisfy consumer needs and increase profits. Thus, consumer requirements are reconciled with the economic imperative. The corollary is that hurting consumer interests can lead to a depression of profits. Therefore, consumer-friendly technical installations should be desirable, not in order to demonstrate excessive civil responsibility on the part of the media industries and concede to consumers their well-deserved legal freedom. Instead, the idea is to selfishly maximize profits by accounting for the needs of honest and potentially illicit consumers.

Paradox of profitable piracy

The pirating of copyright materials is considered harmful to the interests of the copyright owner. However, some economists argue that the toleration of certain levels of piracy can enhance profits and accommodate consumer demand for more liberalized usage, a position which may appear counterintuitive at first sight. Three factors associated with "profitable piracy" have been identified in the economic literature: indirect appropriation, experience effects and network externalities (King and Lampe 2002).

In the case of *indirect appropriation*, the copyright owner is able to obtain revenue from unauthorised copies by charging a higher price for the original media products from which unauthorised copies are made. The logic behind this approach is straightforward: If the copyright owner knows which originals will be used to make copies, a higher price can be charged for these originals. This allows the copyright holder to capture some of the revenues that could have been appropriated through ordinary sales if unauthorised copying had been prevented (Liebowitz 1985).

Experience effects can also lead to profitable piracy. Information goods can be considered to be experience goods, since consumers are not perfectly informed about the characteristics of media products prior to consumption. Copies provide information concerning the

value of a product, and this in turn promotes the purchasing decision. Network technologies, such as Peer-to-Peer (P2P) systems, can help copyright owners by making it easier for consumers to inspect the media products (e.g. by sampling songs), so as to facilitate the purchasing decision. If P2P systems were merely used to "try out" content, then their use would be complementary to retail purchasing, rather than a substitute for it. In addition, the exchange of media products stimulates demand by allowing consumers to sample content that is subsequently bought.

Finally, *network externalities* are highly relevant in markets for information goods in cases where consumer valuation of a good increases when more consumers have purchased it. For example, in the case of online games, network effects emerge from the liquidity of the player pool. Both legal and illegal copies of the game application can expand the "network" of consumers of that online game. Due to the existence of network effects, unauthorised copying and consumption provide value to legitimate buyers. It thus seems reasonable that illicit copying may benefit rights holders for information goods that exhibit network effects (Conner and Rumelt 1991).

Effects of content degradation

Media companies can also engage in content degradation activities, by focusing on ways to increase the utility difference between original and pirated products. An important parameter is the degradation factor that represents the utility discount of the media product vis-à-vis the original product. A low degradation factor means that the pirated product is only slightly degraded and provides almost the same utility to the consumer as the original product. Conversely, a high degradation factor reflects substantial degradation and consequently a significant loss of utility vis-à-vis the original product. The concept of content degradation can be interpreted in two ways:

First, it can be interpreted as the quality discount of the pirated product in relation to the original product. In the case of analogue reproduction, copies represent poor substitutes for originals (e.g. "screener" copies produced illicitly in cinemas). Although this does not apply to digital reproduction, original content often provides consumers with a higher level of utility, to the extent that it is bundled with valuable additional services, which are unobtainable or difficult to obtain from pirates. For instance, software products are often supplied with manuals and support services, such as technical support; and discounts on upgrades may be provided.

Alternatively, it can be interpreted as a transaction cost disadvantage incurred when purchasing the product from a pirated source. In this interpretation, a high degradation level means that the transaction cost is prohibitively high when purchasing from a pirate, with the result that the valuation of the original media product is reduced almost to zero. For example, in the case of highly degraded media product, a consumer who wishes to purchase from an original content provider can simply buy the content legally via a known (online) retailer. If instead the customer wishes to purchase from the pirate, it is first necessary to find the pirated product, which implies higher search costs and possibly greater download costs than in the case of purchasing the original product. Thus, the overall transaction costs of purchasing from a pirate may be much higher than are those for purchasing from a legal source. This reduces the level of utility of pirated products.

Content degradation strategies

Content degradation strategies assume that the media company can determine the level of degradation of competing pirated products. While network effects are inherent in a media product and therefore constitute a given exogenous parameter, it can be argued that the quality difference between a pirated product and the original is something that can be deliberately designed into the competing products. In fact there are at least three strategies which could cause customers to have a reduced willingness for pirated as opposed to original products (Ünlü 2005).

First, media companies can combine their information products with (physical) services that are difficult to copy. For example, this could take the form of more sophisticated (including individualised) artwork accompa-

nying audio CDs, or bundling media products with promotional activities, such as sweepstakes.

Secondly, media companies could increase transaction costs for illegal purchases. One approach would be for legal companies to penetrate P2P networks and supply illegal downloaders with fake pirated goods. This would greatly increase the search costs involved in finding genuine pirated goods. This has occurred in the case of *Madonna*'s "American Life" album, where fans seeking tracks from P2P networks have downloaded files which are blank except for Madonna delivering a message to those attempting to download her new songs. This could at least provide a fresh approach to the problem of music piracy and file-trading.

Thirdly, through fear campaigning, media companies could highlight the ethical and legal problems associated with piracy. This could result in a psychological devaluation of pirated media products.

It can be seen that there are various ways to deliberately increase the degradation level, which can also be used in combination. In all these cases, media companies have to incur additional costs in order to increase the utility difference between original and pirated products. Related costs include production costs for additional physical components, server and broadband capacity to infiltrate P2P networks, and advertising costs.

The benefit of "homemade" content degradation is that it reduces the need for technical protection. This means that content degradation is in some sense a substitute for a higher protection level. Therefore, with a bundle of degradation measures, the need for high-security, illiberal DRMS can be reduced. Honest consumers are not hurt but – instead – benefit from this downward adjusted level of protection. However, efforts to increase the quality difference between original and pirated products (e.g. by means of content individualisation) also imply costs which should not be unreasonably high (Ünlü 2005).

Bottom line

The aim of this article was to demonstrate that consumer and media industry interest must not diverge. On the contrary, optimised profits can only be achieved by accounting for consumer welfare. Specific characteristics of markets for information goods (which exhibit network effects) must be taken into account when deciding on an appropriate level of copyright protection. Besides, product design decisions can add value to products confronted with piracy, when such measures are a cost-effective alternative to technological protection measures. Based on theoretical evidence, there is reason to suggest that media managers should be careful not to implement excessively high levels of protection. Consumer interests have normative implications for the ideal design of a DRMS. In future, further research efforts should be made to investigate the interrelationship between consumer utility and the need for technical protection from an economic perspective.

Sources

- Bechtold, Stefan (2002): Vom Urheber- zum Informationsrecht. Implikationen des Digital Rights Management. Beck, Munich
- C.S.a.T.B. (Computer Science and Telecommunications Board) - National Research Council (2000): The digital dilemma - Intellectual property in the information age. National Academy Press, Washington D.C.
- Clark, Charles (1996): The publisher in the digital world. In: Proceedings of the joint ICSU-UNESCO international conference on electronic publishing in science. UNESCO Publish, Paris
- Conner, Kathleen R.; Rumelt, Richard P. (1991): Software piracy: An analysis of protection strategies. In: Journal of Management Science 37 (1991) 2, pp. 125-139
- King, Steven P.; Lampe, Ryan (2002): Network externalities and the myth of profitable piracy. Intellectual Property Research Institute of Australia (IPRIA), Working Paper No. 03/02, University of Melbourne, Melbourne

- Liebowitz, Stan J. (1985): Copying and indirect appropriability: Photocopying of Journals. In: Journal of Political Economy 93 (1985) 5, pp. 945-957
- Shapiro, Carl; Varian, Hal (1999): Information rules: A strategic guide to the network economy. Harvard Business School Press, Boston
- Ünlü, Vural (2005): Content protection – Economic analysis and techno-legal implementation. Herbert Utz, Munich
- Ünlü, Vural; Hess, Thomas (2004): Functional reference model for Digital Rights Management Systems. In: Proceedings of the 15th ITS Conference, Berlin
- Ünlü, Vural; Hess, Thomas (2005): The access-usage-control-matrix: A heuristic tool for implementing a selected level of technical content protection. In: Proceedings of the seventh international IEEE conference on e-commerce technology, p. 512 – 517
- von Walter, Benedikt; Hess, Thomas (2004): A property rights view on the impact of file sharing on music business models. In: Proceedings of the 10th AMCIS, New York
- Yoon, Kiho (2001): The optimal level of copyright protection. Korea University, Department of Economics, Seoul

About the author: Dr. *Vural Ünlü* is Managing Partner of Cogitans Consulting GmbH that has been delivering consulting services to the top-management level of telecommunications, media and entertainment industries since 2001. He has investigated the domain of Digital Rights Management Systems from a multidisciplinary perspective in the Institute for Information Systems and New Media (WIM) at the Munich Graduate School of Management (LMU München) and is author of the book "Content Protection – Economic analysis and techno-legal implementation". Vural can be contacted at vural.uenlue@cogitans.de

Status: first posted 20/10/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=148

Magnatune - A voluntary-based model for online music

By: Tobias Regner and Javier Barria, Imperial College London, United Kingdom

Abstract: The article analyses the behaviour of consumers of the online music label Magnatune. Its online store allows users unlimited streaming. This comprehensive pre-purchase access facilitates music discovery and allows an informed buying decision. Consumers may pay what they want for music albums as long as the payment is within a given price range ($ 5-$ 18). Our empirical analysis shows that the average payment is $ 8.20, far more than the minimum of $ 5 and even higher than the recommended price of $ 8. We conclude that Magnatune's open contracts design can encourage people to reciprocate and make voluntary payments.

Keywords: economic analysis – business models, consumer behaviour, economic theory, music markets

Introduction

Social preferences have been increasingly studied in theoretical and empirical research. We develop a social preferences-based model to analyse the music industry which struggles to adjust its conventional business model to the challenges of P2P file sharing networks. Conventional online music stores attempt to implement Digital Rights Management (DRM) systems in order to stop illicit copying. However, effective copy protection appears to be hard to achieve as P2P file sharing still thrives. Moreover, common DRM systems restrict consumers in their consumption in various ways (limitations on sampling, burning or transferring content).

The niche label Magnatune (cf. sources) goes another way. It lets consumers choose from a given price range ($ 5 to $ 18). They can pay what they want for music. Moreover, Magnatune offers a free and comprehensive music discovery tool. An online radio service

with unlimited streaming lets consumers try out songs they are interested in. We collected a data set of all the label's transactions over 18 months and analysed the payments that consumers made.

The results of our investigation of this alternative business model – the variable pricing concept of Magnatune – are presented in the following. First we describe Magnatune in detail; next we introduce our theoretical model and highlight the findings of our data analysis. Finally we draw conclusions from the research performed. The complete theoretical model and the full regression analysis of the data can be found in an extended paper (Regner and Barria 2005).

The music label Magnatune

The label was founded in October 2003 and it has around 200 artists on contract. Magnatune prides itself of having a very strict selection process to guarantee high quality. The revenue is evenly split between artist and Magnatune and its slogan is: "We're a record label. But we're not evil." File quality and format is up to the consumer. Even CD-quality files can be downloaded and the formats on offer give a good choice: WAV, MP3, OGG, FLAC and AAC. The payment is variable as consumers can set the price themselves. The given price range for an artist's album is $ 5 to $ 18 and Magnatune recommends $ 8. The actual price is selected by the consumer in a pop-up menu where $ 8 is the default setting.

Payment is processed by credit card or PayPal. As it is not compulsory to leave an e-mail, consumers can remain anonymous at Magnatune. Albums can be downloaded online or bought as a CD. A fee ($ 4.97) for the physical costs of material and shipping is due for CD purchases. Magnatune is based in the USA, but as an online store it has consumers around the world.

Magnatune's artists are categorised in various different genres. There is a wide range of music available from classical music to Electronica, Jazz and Blues, Metal&Punk, New Age, Rock and Pop, World and several more. Magnatune can be seen as a niche label that offers music of relatively unknown artists. Mainstream music of famous artists is not sold. Therefore, the focus of Magnatune – and the article's – is music of less-known artists and subsequently uncertain quality.

Experience good aspects are well taken into account at Magnatune as music discovery is greatly facilitated. Full streaming access to all songs is provided in low or high quality. An online radio service can be used to listen to genre selections or artists' albums. Visitors of the site are allowed to test the available music as often as they want. Essentially, consumers have all possible means available to sample music and find out how much a song/album is worth to them before having to make a decision on the payment. This stands in stark contrast to the usual practice of conventional online music stores where merely 30 seconds snippets of songs are available for sampling if at all.

Summary of the model

We studied the relationship between labels and consumers using a moral hazard model for our analysis. It takes social preferences (see Camerer 2003) into account and it considers the importance of free sampling of experience goods (e.g. music). Magnatune's comprehensive pre-purchase access allows consumers to make an informed buying decision. They can experience the information good long enough to determine how much it is worth to them and decide whether they really want to buy it. This full pre-purchase access can also be regarded by consumers as kind behaviour of labels (as it allows them to make an informed choice). Consumers are willing to reciprocate by making a high voluntary payment, if they are socially-minded. Selfish consumers would free ride and would only pay the minimum.

In the model the label offers music online on its web site and consumers purchase albums. The payment of consumers is not enforceable as substitutes are available for free in P2P file-sharing networks. It is therefore subject to moral hazard. Moreover, the value of consumption depends on the amount of pre-purchase access to music. Limited access and restricted sampling mean a lower value for consumers than comprehensive pre-purchase access.

In contrast to a conventional label the set up of Magnatune allows for an open contracts design. The agents have the opportunity to respond to the action of the other. Thus, both sides are encouraged to reciprocate. Fairness and reciprocity can also be regarded as the enforcement device of this contract (see Fehr et al. 1997 for a similar model in a labour market context). The fact that the consumer in our model is free to choose the payment from a given range adds this feature to the contract design. Hence, our model consists of two stages. First, the label decides whether it allows free comprehensive pre-purchase access to the music or not. Then, the consumers make their purchase and payment decision (being kind, e.g. a voluntary payment, or not).

The theoretical model explains when consumers make a voluntary payment. Social preferences are incorporated into the utility function with a reciprocity payoff. This applies the psychological game theory framework developed in Geanakoplos et al. (1989) and is based on the seminal work of Rabin (1993) and Dufwenberg and Kirchsteiger (2004). The utility function of socially minded individuals increases not only in their material payoffs but also in the psychological payoffs which depend on the individuals' kindness to others and beliefs about that. Essentially, utility increases when the signs of kindness and beliefs about the other's kindness match. Two equilibria – a negative reciprocity equilibrium (both playing nasty) and a positive reciprocity equilibrium (both playing kind) – are possible. Consumers will prefer to make a voluntary payment once reciprocity gains outweigh the material loss of making the higher payment. However, consumers and label have to be sufficiently motivated by reciprocity for this to happen.

As concerns for reputation do not play a role in this context we conclude that the premium exceeding the minimum price of $ 5 should be motivated by social preferences, e.g. reciprocity.

Data analysis

Our data set goes back to the actual start of Magnatune's service in September 2003 and contains all 14,367 album purchases from then until January 2005. Upon initial contact Magnatune was interested in research collaboration and hence provided the data. Apart from the payment information we also collected the purchase date, an encrypted identifier of the consumer, his/her gender and country of residence, the artist, the music genre, the means of payment, the type (download or CD) and whether an e-mail address was left or not. In addition to these variables we computed the total amount of purchases and the number of a respective purchase of a consumer. Moreover, we created a dummy variable for female consumers, if no e-mail was left, if a CD was purchased, if PayPal was used and also various country and genre dummies. The number of purchases has been fairly stable over time and there is only minor fluctuation since October 2003.

The average payment for an album is $ 8.197, the median and mode of the distribution are both $ 8. Only 14.5% of all purchases were at the required minimum of $ 5. No time trend can be seen during the observation period. The data has been generated by 7,620 different consumers; most of them (4,986) purchased only one album. On average consumers bought 1.86 albums. The most albums a consumer purchased were 49. Payments made vary between the minimum of $ 5 and the highest price possible.

Further interesting findings are: Consumers who leave an e-mail tend to spend more on a purchase. The average payment is $ 8.23 when consumers left their e-mail, while it is $ 7.82 when consumers preferred to remain anonymous. The two payment options credit card ($ 8.21) and PayPal ($ 8.16) average very similar payments. CD buyers pay a fee ($ 4.97) for the physical costs of material and shipping. Still, the sale of CDs ($ 8.93) generates a higher payment than the sale of downloadable files ($ 8.17). About two thirds of sales come from the U.S. After correcting for currency and GDP differences between countries only minor variations in the size of payments can be observed.

The average payment decreases with the total of purchases a consumer has made. While the average payment for one-time purchases is $

8.29, the average payment with more than four purchases is only $ 8.06. There seems to be a decreasing individual trend line for frequent consumers. However, the average payment of first-time buyers is stable around $ 8.26 and they are also "joining" Magnatune at a stable rate over the months.

Conclusions

Our model explains the behaviour of Magnatune consumers who consistently pay more than the requested minimum price and even pay more on average than the recommended/default price. We conclude that reputation effects cannot play a role in this environment. Therefore, social preferences are the likely motivation of the consumers that make voluntary payments.

Reciprocity is the source of social preferences in the model. The comprehensive and free pre-purchase access of Magnatune allows consumers to make an informed buying decision. This is regarded as kind behaviour by sufficiently socially-minded consumers and it triggers a kind reaction. They make a voluntary payment, while self-interested consumers only pay the minimum. All consumers do maximise their utility.

Our empirical analysis shows that the average payment is $ 8.20, far more than the minimum of $ 5 and even higher than the recommended price of $ 8. A regression analysis shows that several factors have an impact on the size of the payment. The purchase of a CD (instead of the mere download) has a positive effect as well as some genres, e.g. "rock". The number of purchase and the anonymity of the consumer affect the payment negatively. The dummy for female consumers is not significant.

Compared to a conventional online music store that charges a fixed price of – for instance – $ 8 an album (and offers only limited sampling possibilities if at all) Magnatune makes more visitors acquainted with its songs and thus turns more visitors of the site into consumers; and they still pay more than the recommended price of $ 8.

Bottom line

Still, despite the positive results of voluntary contributions and variable pricing for music it is important to stress that a niche of the market has been analysed and the results for rather unknown artists cannot be easily applied to the mass market. Nevertheless, the open contracts design of Magnatune should be regarded as a promising alternative to strictly DRM-based stores. In an artist life-cycle model it suits artists in an early stage where they are not (yet) well-known. Then, the experience good aspect of pre-purchase access and the higher exposure it allows is relatively more important.

Sources

- Camerer, C. (2003): Behavioral game theory: Experiments in strategic interaction. Princeton University Press, Princeton
- Dufwenberg, M. and G. Kirchsteiger, G. (2004): A theory of sequential reciprocity. Games and Economic Behavior, 47, pp. 268-298
- Fehr, E.; Gächter, S.; Kirchsteiger, G. (1997): Reciprocity as a contract enforcement device: Experimental evidence. Econometrica, 65, 833-860
- Geanakopolos, J.; Pearce, D.; Staccetti, E. (1989): Psychological games and sequential rationality. Games and Economic Behavior, 1, 60-79
- Magnatune: http://www.magnatune.com
- Rabin, M. (1993): Incorporating fairness into game-theory and economics. American Economic Review, 83, 1281-1302
- Regner, T. and Barria, J. A. (2005): Magnatune: Variable pricing for music, mimeo, online available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=721596

About the authors: *Tobias Regner* is a research associate and Javier Barria a senior lecturer at Imperial College London. They have extensive research background in the economics and business aspects of digital media industries. Javier Barria has also been work package leader in several EU-funded projects. The current projects TIRAMISU and DANAE partially supported this work. Both authors are based in the Intelligent Systems & Networks group of the Department of Electrical and Electronic Engineering, Imperial College London, Exhibition Road, SW7 2BT, London, United Kingdom. E-mail: t.regner@imperial.ac.uk and j.barria@imperial.ac.uk

Status: first posted 20/10/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=147

Can TPMs help create a commons?

Looking at whether and how TPMs and Creative Commons licenses can work together

By: Jordan S. Hatcher, JD - Austin, Texas

Abstract: The Common Information Environment (CIE) recently released a report concerning the possibility of using Creative Commons licenses for information produced by public sector bodies (Barker et al. 2005). One of the issues that came up during the study was the compatibility of Creative Commons (CC) licenses and Digital Rights Management technologies (referred to here as Technical Protection Measures). Many public sector bodies felt that password protection schemes were a practical necessity and would not consider CC if they could not place materials behind a password. This article expands upon the conclusion in the report that CC licenses do allow password schemes and considers a broader scope of TPMs. Though any organization or individual looking to implement TPMs on CC licensed content must tread carefully, TPMs can be used to enhance the attractiveness of CC licenses.

Keywords: technical analysis – Creative Commons, public sector, technical protection measures, watermarking

Introduction

This past summer, the Common Information Environment (CIE) group – a collection of public sector organizations that work together to provide information services to UK citizens – sponsored a study into the applicability of Creative Commons (CC) licenses to UK public sector organizations. Under this study, Intrallect and the AHRC Research Centre for Studies in Intellectual Property and Technology Law at the University of Edinburgh examined "the potential for Creative Commons licenses to clarify and simplify the process of making digital resources available for re-use". The public sector organizations concentrated on in the study included museums, libraries, and teachers from all levels of education. Any public sector body, however, could apply the information in this report (and in this article) with, of course, taking into consideration laws such as the recent *Directive on the re-use of public sector information* (Directive 2003/98/EC).

Copyright issues can often hinder sharing between organizations and by end-users. Take, for example, a teacher who wants to create a set of handouts and a PowerPoint for a class on 20th century Spanish art. There are, perhaps, 10 other teachers that have taught this same class. In order to assist in creating her class, this teacher would like to build on some of these other materials and to include some pictures of the artwork. Copyright law states that she will need to get permission from each author – which means contacting each artist and teacher (and possibly their institution) and getting written permission to use the materials. This process of asking permission can be very time-consuming and most teachers will either use the materials without asking (infringement) or not use the materials at all. This creates a major stumbling block to an organization aimed at literally creating a "Common Information Environment" where information can be freely shared. Licenses such as the ones offered by Creative Commons are seen as potentially solving these problems essentially by labelling the content as "shareable" and therefore removing the need for end-users to go through the tedious process of asking permission.

Through stakeholder workshops conducted as part of the study it quickly emerged that Technical Protection Measures (TPMs) may be both desirable and potentially a problem

under the terms of the Creative Commons suite of licenses. At first blush the two may seem too incompatible at all to work together: CC encourages openly and freely sharing material while some see TPMs as restricting sharing. The key to resolving this superficial conflict resides in realizing the true scope of CC licenses and TPMs. Creative Commons licenses, do not simply allow a free-for-all among users. There are certain limits and responsibilities on behalf of the user, such as non-commercial use restrictions in the CC-NC license or attribution requirements. As any reader of the INDICARE Monitor will surely know, TPMs don't mean total control. Consumer perception, however, often equates TPMs with severe restrictions. Thus some clarification of how CC licenses and TPMs can work together is in order.

This article first takes a look at the problems and needs of end-users. This section identifies possible areas where TPMs may be a solution to some of the misapprehensions that organizations may have in using Creative Commons licenses. The next section then looks at the license itself to see the possible TPMs that organizations could use and still remain compliant with the license. The next two sections deal with two different kinds of TPMs, those that deal with access to the work versus those that deal with the work itself. The article then briefly concludes with a word of caution about some of the solutions in this area.

Problems and needs of end-users

Several questions and problems arose during the course of the study where technological measures were identified as being either useful or essential to end-users in order for them to feel comfortable with using Creative Commons licenses. These areas primarily concerned:

- **Authenticated Environments** – Many participants were interested in placing CC-licensed materials in such authenticated environments as intranets, virtual learning environments, and digital repositories. The practical difficulties of separating out CC-licensed material from restricted access material proved the most major stumbling block when considering these licenses. If the licenses prohibit use of the material behind a password (authentication), then most institutions would not use Creative Commons simply because of the extra expense of maintaining a separate access system (website, database, etc).
- **A desire to track use of the work** – Many groups would like to see how their works are being used both for grant purposes, such as to report back to funding organizations on the effectiveness of a project, and to be able to assess their own effectiveness.
- **Preventing commercial use** – There was a significant interest (67%) (Barker et. al. 2005, p. 11) in the Non-Commercial license option and thus an interest in ways to maintain this restriction.
- **Guaranteeing integrity of the work** – Many participants were concerned about the reputational harm caused by end-users altering their works in unacceptable ways. A way to guarantee the integrity of the work was seen as desirable in order to prevent this harm

The last three areas deal with technological measures directly affecting the works, while the first area only considers measures that control access to the area where the work is stored. The next step is to examine the licenses themselves to see if these four areas may be used within the terms of the license.

Terms in the Creative Commons

The Creative Commons movement started in the United States and has evolved into a worldwide phenomenon. The goal of the licenses is to provide a simple way for users to allow others to share their works in a "some rights reserved" environment. Instead of hiring a copyright lawyer or going through the tedious process of drafting their own license, users can go to one of the Creative Commons websites and click through various options to arrive at a license. A wealth of information is available on their site and within the CIE report about the different options available, and readers are encouraged to find out more through these sources.

Despite the different options, such as the Non-Commercial restriction mentioned above, each license is made up of a set of "baseline rights" that are a part of every license. The language addressing Technical Protection Measures is in this section. The first question is to consider what TPMs the Creative Commons licenses prohibit. In regards to TPMs, the generic license states:

> 4. Restrictions ***
> a. *** You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work *in a manner inconsistent with the terms of this License Agreement*. (2.5 BY)

Jurisdiction specific licenses such as the England and Wales licenses or the German licenses are ported from the generic license; therefore the generic license is the focus of this article. The emphasized portion quoted above demonstrates that CC licenses only prohibit TPMs that change the rights granted by the license.

Because these licenses only bar TPMs that alter or restrict the terms of the license, the next step is to pinpoint the rights are granted by the license. The baseline rights also contain the following grant to the end-user:

> 3. License Grant. ***
> a. to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;
> b. to create and reproduce Derivative Works;
> c. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;
> d. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission Derivative Works. (2.5 BY)

Obviously the sections granting derivative work rights are altered and new language is added in licenses with the "No Derivative" option. Besides the above grants, there are additional restrictions, such as "keep[ing] intact all copyright notices" and requiring attribution of the work. When these two parts of the license are read together, it seems that there is significant room for TPMs to work in the Creative Commons environment. The CC website even mentions that TPMs can be used with the licenses (FAQ, 5.12 and 5.13).

Authenticated environments

Password protected or otherwise authenticated environments are probably the easiest area to address when examining TPMs and Creative Commons. Examples include intranets, virtual learning environments (VLE) (online classes), and digital repositories (such as for teaching materials). These environments need to be authenticated because they require access to copyright restricted material, such as licensed textbook material in a VLE. These passwords are contemplated only to gain *access* to the storage area of the work and not placed on the work itself. Placing a password on the work itself, such as can be done in Adobe when creating *.pdf files, would be both unnecessary and would violate the terms of the license by restricting the ability to reproduce and distribute the work.

Authentication schemes are based more on practical necessity and not on a desire to restrict certain uses of the works. As a result, the institutions involved do not have a desire to prohibit any of the granted rights inside or outside of the password system. End-users would still be free to distribute or reproduce the work both inside *and* outside the password-protected domain. Clearly, any attempt to restrict them from taking CC-licensed work outside of the authenticated environment would contravene the rights granted by the license (distribution, reproduction, etc.). Based on this, Creative Commons licenses do not restrict institutions from placing materials inside of an authenticated environment. Care would have to be taken by organizations using password schemes that they do not include terms in the contract for registra-

tion that violate the CC license (such as forbidding distribution outside of the system) or in the case of Non-Commercial CC licenses try to make commercial use of the user registration or use data gathered within the system.

"Direct" TPMs

Technical Protection Measures that cover the three other areas mentioned – guaranteeing integrity, tracking use, and preventing commercial use – all involve TPMs attached to the actual works themselves. Again, using Adobe as an example, users *could* create *.pdf files that prohibit printing or copying portions of the work, but features such as these would plainly violate the terms of the license. Exactly what types of TPMs comply with CC licenses is outside the scope of this article, but one in particular is worth mentioning: Watermarking.

Watermarking, like the password protection schemes mentioned, is the least invasive method and thus most likely to comport both philosophically and legally with the Creative Commons family of licenses. Simply placing some information in the work would not hamper the ability to copy and distribute the work. They would perhaps be most useful for those using the "No Derivative" CC license. Watermarking could allow for users to authenticate the integrity of the content and for content creators to track use. The use information can then be passed on to funding agencies or used internally in order to assess the usefulness of the licenses in encouraging re-use. These watermarks could also help prevent commercial use for organizations using the non-commercial (NC) option.

TPMs placed directly on the works tread a fine line between allowing the freedoms granted under the license and the law (such as fair use/fair dealing) and the goal of limiting use of the work through technical means. Creative Commons as an organization takes a stance against using these technologies because they believe that this line is too fine. From their website:

> Why don't we use technology to enforce rights? ... Perhaps the most familiar is the fact that technology cannot protect freedoms such as "fair use." ... [M]ore importantly, we believe, technological enforcement burdens unplanned creative reuse of creative work. ... [W]e ... are concerned that the ecology for creativity will be stifled by the pervasive use of technology to "manage" rights. ...[W]e prefer [copyrights] be respected the old fashioned way - by people acting to respect the - freedoms, and limits, chosen by the author and enforced by the law. (FAQ 5.12)

Use of TPMs fits more into a "rights heavy" framework, whereas CC tries to make works easily and readily accessible to users. Organizations need to assess their goals for use of CC licenses and the possible impact of TPMs on re-use by the end-user before implementing any TPM.

Bottom line

Public sector organizations have different needs than individual authors. Thus, they may have more of a desire to use TPMs when making their content freely available. Creative Commons offers a host of licenses that allow the use of TPMs and make content freely available and therefore are an option. Certainly no matter what an organization decides about whether to use TPMs on the CC-licensed work within their control, great care will have to be taken so as to make sure that the license grants are respected. But rather than detracting from Creative Commons licenses, TPMs could enhance the attractiveness to a variety of public sector organizations, including schools, museums, and libraries.

Sources

- Barker, E; Duncan, C; Guadamuz, A; Hatcher, J; Waelde, C. (2005): The Common Information Environment and Creative Commons; http://www.common-info.org.uk/news/archives/2005/10/suitability_of.html
- Creative Commons FAQ: http://creativecommons.org/faq
- Creative Commons Licenses: http://creativecommons.org/licenses/

- Directive 2003/98/EC on the re-use of public sector information; http://europa.eu.int/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf

Acknowledgement

Part of this article has been previously published as an appendix to Barker et al. (2005).

About the author: *Jordan S. Hatcher*, JD recently spent the past year at the AHRC Research Centre for Studies in IP and IT Law at the University of Edinburgh. While there, he participated in the CIE report that is the subject of this article. He currently resides in Austin, Texas, where, among other things, he serves as a board member and officer for EFF-Austin, a Texas-oriented cyber-liberties group. He can be contacted at jordan _at_ twitchgamer dot net and at his corner of the web, http://twitchgamer.net

Status: first posted 19/10/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=146

Virgin Media versus iTunes

Using competition law as tool to enforce access to DRM … and failing

By: Natali Helberger, IvIR, Amsterdam, The Netherlands

Abstract: Apple's tight control over the FairPlay DRM system has caused many iPod users to complain that they cannot play certain files on their iPod, namely the files they bought from other online services, using a different DRM system. The proprietary control over FairPlay is also a thorn in the flesh of iTunes rivals who sought various ways to get around FairPlay's lack of interoperability. The French enterprise VirginMega tried it the legal way - and so did it come that Apple's FairPlay was probably also the first case in which a competition authority in Europe had to decide if access to a Digital Rights Management system can be enforced on grounds of competition law.

Keywords: legal analysis – competition, court decision, DRMS, law suit, standards – France

Introduction

Thanks to the early market instinct of iTunes, the success of the iPod, and the fact that the iPod does not play (DRM-protected) music other than FairPlay protected music, iTunes FairPlay DRM is a desirable resource for many of iTunes' competitors. Part of a clever business strategy, the iPod is able to play all files bought through iTunes and non-protected MP3 files from various (legal and illegal) sources, making it an attractive device for consumers. What the iPod does not do is to support any of the rivalling standards used by competing commercial download services, neither is it particularly willing to license FairPlay to rivals. In other words, Apple faces consumers with the choice: "Are you with us or are you with them?"

In response, there have been various attempts to get around Apple's refusal to licence FairPlay, so that competitors could make their services/devices compatible with the popular iTunes standard. RealNetworks, for example, one of Apple's arch enemies, tried it with reverse engineering and sold music downloads for the iPod in its own unlicensed version of FairPlay . Apple changed its technology and threatened to file suit against RealNetworks (Bangeman 2004). Subsequently, RealNetworks changed its strategy and launched the "Freedom of Choice" campaign to mobilise consumers against the rival's business methods and services. Goal of the campaign was, so RealNetworks, to help consumers "break the chains that tie their music device [iPod] to proprietary music downloads". And, according to RealNet-

works, "We are here to inform AND motivate" (Realnetworks 2004). Having said that, it is obvious that RealNetworks' motives were not purely altruistic. RealNetworks understood very well that a combination of successful hardware and a proprietary software standard can be a very successful strategy to exclude unwanted competitors, such as RealNetworks, from one's customer base (here: the large iPod population). Or to extend one's own customer base: this is what Microsoft is trying with its own Media Player technology which is offered at favourable licensing conditions to music services and device makers, thereby seeking to outdo Apple.

The French entertainment company VirginMega tried another way: the legal way. It filed in 2004 a complaint against Apple Computers France with the French competition authority, the Conseil de la concurrence (Conseil de la concurrence 2004). VirginMega offers its own music download service and uses for this purpose a different DRM solution, namely Microsoft's DRM. Because of the proprietary nature of the iPod, consumers who buy digital music files from VirginMedia cannot, thus the argument of VirginMega, transfer these files to their iPods. VirginMega requested a licence from Apple for FairPlay so that it could encode its music files in the FairPlay format. Apple refused. VirginMedia claimed that the refusal to grant access to the FairPlay DRM constitutes an abuse of a dominant position according to French competition law and Article 82 of the EC Treaty – and that is where the case became interesting for lawyers and the legal-minded. The goal of this article is to report about the decision – in a shortened and rather simplified version (for an extensive discussion, see Helberger 2005) - and the arguments that the French competition authority used to deny the request.

The infamous Essential Facilities Doctrine

The French competition authority examined the access request of VirginMega and recalled for this purpose the jurisdiction of French courts and the European Court of Justice in so called Essential Facilities Doctrine cases. Some words of explanation are in place.

Article 82 (a) of the EC Treaty contains a broad general principle that stipulates that companies in dominant positions must not refuse to supply their goods or services if refusal to supply would significantly impact competition. Having said this, the granting of access to a facility goes beyond the mere duty to supply. The obligation to share one's own assets with competitors can result in considerable conflicts with commercial interests and economic freedoms, including the right to property and the freedom not to be forced to promote competitors at one's own cost (European Commission (1987), European Court of Justice (1998) and (1995), to name but some). In addition, the sharing of one's resources can trigger considerable security risks for the resource operator, as well as capacity problems and additional costs. All these are reasons why the European Court of Justice, the European Commission and scholars have argued that the obligation to share one's resources should remain subject to stricter conditions those foreseen by Article 82 (a) of the EC Treaty. Access obligations should be reserved for exceptional circumstances, which are summarised in the so called Essential Facilities Doctrine. The Essential Facilities Doctrine has been proclaimed by some scholars as a "powerful tool to pry open markets" (Furse 1995), while it has been viewed rather critically by others.

The Essential Facilities Doctrine says that any dominant company that controls a so-called "essential facility' and that refuses access to competitors without objective justification or that grants access only on terms less favourable than those that it offers its own associates, acts in breach of Article 82 (a) of the EC Treaty. An essential facility in the sense of the Essential Facilities Doctrine may be a product, a service, content, infrastructure, technical facilities or access to a physical thing such as a harbour or an airport. In other words, Virgin could stand a chance to force Apple's iTunes to share the FairPlay DRM if (1) Virgin can prove that Apple is a dominant player, that (2) FairPlay is a facility access on which Virgin depends if it wishes to supply its customers with mu-

sic services and that (3) implementing an alternative DRM standard is not an economically viable option. Finally, it would have to (4) demonstrate that certain economic interests of iTunes, concerning available capacity, security, technical standards and reasonable remuneration interests, are accommodated.

The decision of the French Conseil de la concurrence

The decisions of the French competition authority is instructive as it is, to the knowledge of the author, the first time that a European competition authority had to decide about the legitimacy of a refusal to grant access to a DRM standard under competition law. It is interesting to note that the Conseil de la concurrence found that a technology that implements a proprietary standard could constitute an essential facility. In other words, it is not the facility itself but the standard that is embedded in the facility that can make it essential for market entry for others. In the end, it decided against a foreclosure effect, acknowledging that market foreclosure due to control over a dominant DRM standard could not be excluded under different circumstances (see Mazziotti 2005). The competition authority found Apple to be dominant in the markets for portable music players and downloaded music. For this purpose, the agency developed a number of arguments. The Conseil de la concurrence identified three aspects that were in its opinion relevant when deciding whether FairPlay is an essential facility:

- a. The actual usage habits of consumers regarding music download,
- b. Possibilities to circumvent the problem of lacking interoperability, and
- c. The developments in the market for portable music players.

The Conseil de la concurrence concluded that FairPlay was not an essential facility for the following reasons: First, the competition authority found that only a minor share of the market would listen to music from a portable device, the majority would listen to music via the computer or burn songs onto a CD. Second, and rather unorthodoxly, it described in detail a method how consumers could get around the existing lack of interoperability and download music from VirginMega onto their iPod. Third, the French competition authority found that the market for portable music players was sufficiently competitive and offered several portable players in addition to the iPod. In other words, there were alternative players available that could process VirginMega's DRM standard. In conclusion, the French competition authority did not consider FairPlay an essential facility because consumers had a choice: access to the FairPlay standard was not necessary to offer consumers VirginMega's music. It furthermore found that the market for online music was actually competitive as there were at least two major operators active in that market (Conseil de la concurrence, paragraphs 96-103). In addition to its doubts whether the FairPlay DRM was an essential facility, the French competition authority also questioned the causality between VirginMega's lesser economic success and the access refusal. It argued that Apple probably had the more successful business strategy and was for this reason market leader, thereby raising the free-rider issue.

Discussion

Virgin's attempt to call upon competition law to get access to the FairPlay standard failed, at least before the French competition authority. I tend to say: rightly so. Because of its economic implications, the essential facilities doctrine should be applied with caution and be a last resort when competitors are otherwise completely excluded from offering a new service. This is not to say that the present development – segmentation of the music market into a number of competing and non-interoperable DRM standards – is a situation that should be tolerated. Far from it.

The point that I want to make is that because of the many insecurities and difficulties in defining whether its conditions are given, the Essential Facilities Doctrine does not provide potential market players with the legal security that is necessary when launching a new business. Moreover, the application of the Essential Facilities Doctrine to enforce access to a technical standard or interoperability is highly problematic, especially where

such standards are protected by intellectual property rights and trade secrets (see the discussion in Leveque (2005) and Mazziotti (2005). Another argument is that in the competition law analysis, economic reasoning commonly prevails; public information policy considerations about open access and the wide availability of different sorts of content from different sources – non-economic arguments that play an important role in this context – often are not part of the competition analysis, or only to a very limited degree. Arguably, mandating access on a formal legal basis and by way of a constitutional law-making process is the preferable route to strike the needed balance.

A different question altogether is whether mandating access to a particular DRM standard is the solution to the problem of technical market segmentation as far as DRM is concerned. One aspect that is worth being considered in this context is that enforcing access to a particular DRM standard could further re-enforce the dominance of the FairPlay standard and discourage competitors from designing technically more advanced, and more consumer-friendly solutions. Mandated access regimes can be very questionable from the standpoint of static and dynamic efficiencies and consumer welfare. Access obligations could hamper investment by cutting down incentives to invest in technical innovation and improvement, and by discouraging other enterprises from doing so. As a consequence, mandated access could further strengthen the market position of a particular standard rather than remedying it.

Is it paramount for consumers that FairPlay licences its DRM standard to competitors? What probably matters most from the perspective of consumers is that their choice for a particular device does not tie them to one particular service only, but that they are able to switch between different services (see Duft et al. 2005). To this extent, it is the compatibility of the portable player that matters and that should be guaranteed. To realise this goal, one could think of rules obliging controllers of DRM technology to license their technology to the producers of portable players at reasonable and non-discriminatory terms, similar to the rules that now already apply for conditional access controllers in digital broadcasting. One could also think of an obligation to conclude some form of interoperability agreement, e.g. following the model of simulcrypt agreements or common interface solutions that have been propagated for digital broadcasting. Speaking for myself, I would rather purchase a portable device that supports several different DRM standards than download music only from download services that support FairPlay. Am I being irrational here?

Bottom line

The arguments that the French competition authority used do not seem unique to the French music sector. In other European countries, portable music players are also by far not the only way to access music files from online download services, several download services are in competition and different portable music players are available to process their range of music. Another question could be whether the adaptation of the iPod to play additional DRM standards is compatible with national law. Fact is that strict scrutiny must be applied before granting access requests of competitors to a particular DRM standard. The decision confirms standing jurisdiction of the European Court of Justice and national courts that forcing undertakings to grant rivals access to their own resources must remain the absolute exception, and is eventually not even a means to achieve market competition and consumer welfare. Instead, solutions that support the compatibility of consumer devices are probably a more viable route to consider. Useful inspirations could be derived from the regulation of conditional access in digital broadcasting.

Sources

- Bangeman, Eric (2004): Apple responds to RealNetworks' Fairplay hack, http://arstechnica.com/news.ars/post/20040729-4051.html (last visited at 23 October 2005)

- Conseil de la concurrence (2004): Décision du 9 novembre 2004 relative à des pratiques mises en œuvre par la société Apple Computer, Inc. Dans les secteurs du téléchargment de musique sur Internet et des baladeurs numériques, Case No. 04-D-54
- Dufft, Nicole et al. (2005): Digital music usage and DRM. Results from an European consumer survey, Berlin, May 2005; http://www.indicare.org/tiki-download_file.php?fileId=110
- European Commission (1987): Commission Decision of 29 July 1987 relating to a proceeding under Article 86 of the EEC Treaty, (Case IV/32.279 – BBI/Boosey & Hawkes), 9 October 1987, OJ L 286, p. 36
- European Court of Justice (1998): Judgment of the Court of 26 November 1998, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, Reference for a preliminary ruling: Oberlandesgericht Wien – Austria, Case C-7/97, European Court reports 1998, p. I-7791
- European Court of Justice (1995): Judgment of the Court of 6 April 1995, Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission of the European Communities, Joined cases C-241/91 P and C-242/91 P, European Court reports 1995, p. I-743
- Furse, M. (1995): The Essential Facilities Doctrine in Community Law. European Competition Law Review 469, 473
- Helberger, Natali (2005): Controlling access to content – Regulating conditional access in digital broadcasting. Kluwer International: Den Haag
- Lévêque, François (2005): Innovation, leveraging and essential facilities: Interoperability licensing in the EU Microsoft case, Forthcoming in World Competition; pre-print available at http://www.cerna.ensmp.fr/Documents/FL-Ms-WorldCompetition.pdf
- Mazziotti, Guiseppe (2005): Did Apple's refusal to licence proprietary information enabling interoperability with its iPod music player constitute an abuse under Article 82 of the EC Treaty? eScholarship Repository, University of California, http://repositories.cdlib.org/bclt/lts/5
- Realnetworks (2004): Press release http://www.realnetworks.com/company/press/releases/2004/freedom_choice.html (last visited on 23 October 2005)

For a more detailed introduction into the Essential Facilities Doctrine see:

- P. Areeda (1990): Essential Facilities: An epithet in need of limiting principles. 58 (1990) Antitrust Law Journal 841, 852-853pp
- J. Temple Lang (1994): Defining legitimate competition: Companies' duties to supply competitors, and access to essential facilities. 18 (1994) Fordham International Law Journal 441, 478-483pp
- D. McGowan (1996): Regulating competition in the information age: Computer software as an essential facility under the Treshman Act. 18 (1996) Hastings Communications & Entertainment Law Journal 771, 805-806pp

Acknowledgement
Parts of this text are adapted from a recently published book by the author (Helberger 2005)

About the author: Dr. *Natali Helberger* is senior project researcher at the Institute for Information Law, University of Amsterdam, and managing legal partner in the INDICARE project. Dr. Helberger specialises in information law, technical control of information, the interface between law and technology, a between media, intellectual property and telecommunications law. Presently, she is staying as visiting scholar at the University of California, Berkeley. Contact: helberger@ivir.nl

Status: first posted 28/10/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=150

The OECD takes on digital content

By: Philipp Bohn, Berlecon Research, Berlin, Germany

Abstract: The OECD's Working Party on the Information Economy (WPIE) has recently published four extensive reports on digital content. Their relevance for the DRM discussion is analyzed in the course of this article. Where applicable, they are also contrasted with differing findings and positions.

Keywords: review – business models, digital media, DRMS, information economy, OECD

WPIE on digital content

This summer, the OECD's Working Party on the Information Economy (WPIE) released separate reports on digital content in four areas: scientific publishing, music, online computer games and mobile content. They focus on new business models for digital content, changing value chains, growth drivers and barriers, changing market structures and their impact on economic growth and employment (cf. OECD website).

Focus on DRM

The analyses also cover copyright infringement and DRM issues. As could be expected, the reports have been received with mixed emotions. Free market advocates agree that they "do not underestimate the harms of copyright infringement; indeed, they urge the use of so-called 'digital rights management' technology to try to limit piracy. Yet the report cautions that these systems must not crush interoperability among different technologies. Moreover, the OECD worries that technologies may undermine 'fair use' provisions for lawfully excerpting portions of a work" (The Economist 2005).

Content providers follow a deviant agenda. Consequently, *Adrian Strain*, spokesperson for the International Federation of the Phonographic Industry (IFPI), objects: "The report does not recognize the vast proportion of the use of P2P services that is infringing copyright. It fails to acknowledge the extent of the damage that this does to the legitimate industry and oversimplifies the issues surrounding DRM in the development of the online music sector" (Gain 2005).

With one side claiming the reports to be fairly balanced and the other accusing it of oversimplification, I want to take a closer look and discuss what the OECD has to say about DRM.

Scientific publishing

The report describes the industry structure and value chains as well as existing and new business models based on online access. It concludes with challenges and policy considerations. Digital rights management is mentioned only once throughout its 106 pages. Several surveys cited vaguely touch the fields of copyright and access (Accenture 2001, Kraemer et. al. 2002a, E-Business Watch 2002) asking about security concerns, lack of a transparent regulatory framework, inadequate legal protection for purchasers, etc.

However, more than 70 percent of enterprises responding to one survey stated that "goods and services do not lend themselves to selling online" (E-Business Watch 2002). "Given the potential for digital delivery, it is perhaps surprising that unsuitability of goods for online sales should be such a widely cited barrier for media and publishing firms. (…) It may also reflect security and copyright concerns" (p. 50).

The report then introduces the concept of *open access publishing*. Authors following this concept "grant to all users the free, irrevocable, worldwide, perpetual right of access to copy, use, distribute, transmit and display the work publicly and to make and distribute derivative works, in any digital medium for any responsible purpose" (Bethesda Statement of Open Access Publishing 2003). Articles and papers are usually based on publicly funded research. Accordingly, funding agencies and institutions are more

and more adopting the open access policy. Thereby, they are stressing the importance of knowledge creation and distribution and the integration of all the actors and activities within innovative systems. According to the report, DRM does not lend itself to the idea of open access publishing, as it is primarily meant to limit users' rights in terms of openness and interoperability.

These findings are very much in sync with, for example, the interview INDICARE conducted with *Arnoud de Kemp*, who used to be responsible for Springer's digital publishing activities (Springer is a major scientific publisher). According to de Kemp, scientific publishers rely on watermarking at the most. Other, more restrictive approaches would contradict the nature of scientific discourse (de Kemp 2005).

Music

The report starts with a description of the music industry. It also traces changing value chains and business models. A special focus is distribution via P2P networks, including commercial P2P. Also, the impact of online music on artists and consumers is evaluated. The report closes with challenges and policy considerations.

The OECD's position on DRM in the music industry is quite balanced: "Despite their shortcomings, they [DRMs] may be an essential tool to protect intellectual property rights" (p. 94). They supposedly help to tailor content to the consumers' needs and preferences, leading to increased consumer choice and satisfaction. But two of DRM's shortcomings are also addressed: (i) the technology seems to have failed to prevent unauthorised uses, and (ii) increasing use of DRM has raised concern of potentially limiting usage rights.

However, the authors grant that "as opposed to some CD-Rom copy-protection technologies, so far DRMs have rarely been known to prevent legitimate uses of content and services. Still, developers of DRM, players in the market employing DRM, and users of DRM-protected material should be equally concerned to ensure appropriate usage rights, transparency, privacy, as well as ease and reliability of access" (p. 94). The analysis concludes that "one of the first aims should be openness and interoperability" (p. 95).

I agree that openness and interoperability are main issues to be resolved soon. However, I disagree that the restrictions DRM imposes on legitimately downloaded songs are less severe than in the CD-environment. Take for example music downloaded from iTunes – you cannot use them with portable devices supported by Microsoft's DRM and vice versa. The customer should be free to consume music on the device of his choice.

Online computer games

The report to a large degree follows the structure already described for scientific publishing and music. Beyond that, it identifies drivers of the online game industry (technology, demographic factors, venture capital, spillovers from computer games), as well as barriers to its development (broadband coverage and latency, market factors, industry and financial conditions).

Given that musical content mostly is the focus of attention when it comes to digital entertainment, I appreciate the OECD's effort to devote a separate report to computer games. However, DRM is only mentioned once in the 68-page report. The authors name copyright and piracy as one barrier to the development of the computer game industry, "as is the case for all software-related and digital content-based industries" (p. 43).

According to the report, there are some things that make the gaming industry distinct from other digital products such as movies or music: (i) games are not static, with evolving game conditions and players' positions, with two-thirds of programming remaining on the suppliers' servers, leading to (ii) server-based piracy (unauthorised access or copying of content located on servers) as an emerging challenge.

Finally, the question arises of how to handle items that gamers can develop themselves, leading to the issue of *user production rights*. This certainly deserves debate, given the outcome of several cases where digital items have been sold without the original owner's authorisation (BBC 2005; see also Vogeley

2005a and 2005b for a more detailed discussion on DRM and online gaming).

Mobile content

The report on mobile content has a more technological angle and stresses the need for a political framework. It also describes value chains, business models and the general state of mobile content (music, games, video, information, other).

WPIE is right in singling out mobile distribution, because "the mobile environment does pose some additional challenges" (p. 55). On the technical side, the authors identify the Open Mobile Alliance's DRM, Microsoft's Janus DRM and Apple's FairPlay as the relevant regimes.

Asserting that it's the industry's obligation to provide marketable solutions, WPIE also calls for policy makers to take action, following the OECD Council Recommendation on Broadband Development: "Regulatory frameworks that balance the interests of suppliers and users, in areas such as the protection of intellectual property rights, and digital right management without disadvantaging innovative e-business models" (OECD 2004). (The European Commission is also represented in the OECD's Council, its decision-making body.)

In particular, this means that national IP laws must be harmonised and anti-piracy enforcements be coordinated, which has already been recognised by the European Commission. On the business side, key issues include interoperability of DRM technologies and consumer acceptance.

The authors conclude that "IP, DRM and technical standards are essential to continued growth of mobile content. Industry and government-facilitated policies to encourage consensus and development in these areas must also take into account the mobile environment" (p. 61).

Again, I believe that the authors might be a bit too optimistic in assessing the industry's basic willingness to strive for interoperability. Even given pan-European legislative initiatives, DRM-interoperability might still stand in the way of the individual stakeholder's profit maximisation goals. The industry as a whole could so far not agree on a common mobile DRM standard. This is underlined by their inability to come to terms with MPEG LA, the company bundling patents relevant for the implementation of OMA DRM (MPEG LA 2005, see also the GSM Association's response to MPEG LA's revision and Faultline 2005 for further comment).

Bottom line

While the reports taken as a whole are very fair and balanced, taking into consideration the interests of all stakeholders, I disagree on some details concerning DRM, namely in the fields of music downloads and mobile content.

I largely agree with WPIE's assessment of the situation in online gaming and scientific publishing, especially when it comes to open access publishing. Also, I can to some extent relate to both commentators cited in the beginning of the article: the reports rightly stress the overriding importance of DRM interoperability. At the same time and as the authors indirectly admit, DRM-related issues are presented in a slightly oversimplified way: "In sum, the social and economic dimension of DRMs may necessitate further study" (Music, p. 13).

Sources

- Accenture (2001): The unexpected eEurope: The surprising success of European eCommerce; http://www.accenture.com/xd/xd.asp?it=enWeb&xd=ideas\eeurope2001\eEurope2001_home.xml
- BBC (2005): Chinese gamer sentenced for life; http://news.bbc.co.uk/1/hi/technology/4072704.stm
- Bethesda Statement on Open Access Publishing (2003); http://www.earlham.edu/~peters/fos/bethesda.htm
- E-Business Watch (2002): ICT & e-business in the media and printing industries; http://www.ebusiness-watch.org/resources/publishing/SR08-II_Media.pdf
- Faultine (2005): OMA washes its hands of MPEG LA licensing arrangements; http://www.theregister.co.uk/2005/05/05/oma_washes_hands_of_mpeg_la_licensing_agreements/print.html

- Gain, Bruce (2005): Come on music biz, embrace P2P; http://www.wired.com/news/print/0,1294,67820,00.html
- GSM World: MPEG LA's revised terms for digital rights management not acceptable. http://www.gsmworld.com/news/press_2005/press05_15.shtml
- de Kemp, Arnoud (2005): Science can't accept technical barriers of content use! INDICARE-Interview by Ulrich Riehm. INDICARE Monitor, Vol 2, No 6, August 2005; http://www.indicare.org/tiki-read_article.php?articleId=129
- Kraemer, K.L., Dedrick, J., Dunkle, D. (2002a): E-commerce: a mile wide and an inch deep. http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1028&context=crito
- Kraemer, K.L., Dedrick, J., Dunkle, D. (2002b): E-commerce in the United States: Leader or one of the pack?. http://www.crito.uci.edu/publications/pdf/GIT/GEC/USsnapshot.pdf
- MPEG LA (2005): OMA DRM patent holders revise terms of MPEG LA license (press release); http://www.mpegla.com/pid/drm
- OECD (2004): Recommendation of the Council on broadband development; http://www.oecd.org/dataoecd/57/29/32167012.pdf
- OECD website: http://www.oecd.org/document/62/0,2340,en_2649_33757_32160190_1_1_1_1,00.html
- The Economist (2005): Twist and shout – The good and bad of internet file-sharing; http://www.economist.com/PrinterFriendly.cfm?story_id=4066543
- Vogeley, Danny (2005a): The case of Half Life 2; http://www.indicare.org/tiki-read_article.php?articleId=85
- Vogeley, Danny (2005b): Real money for virtual items – A case for DRM?; http://www.indicare.org/tiki-read_article.php?articleId=104

About the author: After having graduated from University of Mannheim (Business Administration), *Philipp Bohn* has joined Berlecon Research as Junior Analyst. He is a member of the INIDICARE-team. Contact: pb@berlecon.de

Status: first posted 21/10/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=149

Editorial of INDICARE Monitor Vol. 2, No 9, 25 November 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: This time the INDICARE Monitor addresses first two hot topics: the Sony BMG XCP copy protection scandal is taken as a starting point to analyse patterns of disproportionate DRM systems and to show that it was not a unique case. Next, an analysis and an INDICARE interview with a Google representative deal with Google Book Search. The analysis reveals the imminent challenge of Google Book Search for the publishing industries, and makes clear why B2B DRM is required to manage the change. The interview focuses on access and usage restrictions of the service and the reasons why. The fourth contribution follows up the progress of European policy towards cross-border licensing for online music. Finally we report about DRM 2005, the fifth ACM Workshop on Digital Rights Management, and close with a review of a sociological research paper on changing boundaries and interrelations of information markets and the public domain in the fields of music and publishing.

Keywords: editorial – INDICARE

About this issue

XCP copy protection & Co

Philipp Bohn investigates three cases of invasive and intrusive DRM systems: Sony BMG's XCP copy protection, StarForce technology, and Microsoft DRM. In all these cases the impact of the technological protection measures is by far disproportionate to the legitimate purpose of DRM systems to enable new business models for digital content. The three cases are rather different with XCP installing a rootkit, with StarForce deactivating burning tools, which can not always be reactivated, and with Microsoft DRM, which may not work correctly after changes to hardware components and may lead to a loss of legitimately purchased property. Despite the differences, there are some common features as the article shows: Intrusive DRM systems tend to be intransparent and prone to create unnoticed security risks. As these systems often have an impact at the operating systems level, they are hard to detect; as they are intentionally hidden, they do not appear clearly addressed in end-user license agreements, and if detected, companies hesitate to admit what they have done. This makes it difficult for consumers to uninstall them. All these hassle-prone DRM systems have a strong taste of consumer neglect and distrust, and can hardly be envisaged as foundations of consumer-friendly e-content services. Furthermore, invasive DRM is hardly compatible with acknowledged principles of ownership, data protection and privacy.

Google Print – Google Book Search

Google Print, renamed Google Book Search, is another hot topic we address in two contributions. *Bill Rosenblatt* shows in an excellent analysis, how Google challenges existing value chains in the publishing business. Today Google Book Search and similar developments are about "discoverability" of publications: "A search engine has the power to expose content as the result of a user's Internet search, direct her to any other resource on the Internet to find the full content… and potentially make money on the referral" (Rosenblatt). While this facility already changes marketing and accessibility of publications, the true disruptive potential is visible just as writing on the wall: rendering of copyrighted works directly on the Internet. This potential has not yet been exploited. To leverage this potential content providers and service providers have to come to terms: "If publishers want to maintain control over their own rights and supply chains in the Internet age, then they will need to take control of their 'rights' and how they make them available to distributors and retailers like Google, Amazon, Yahoo, and MSN" (Rosenblatt). And that's where DRM – B2B DRM to be exact – comes in. Publishers need to define and manage the rights for themselves, decide what rights they are willing to offer to Google and others, and define the standards

for communicating these rights. While this is the main message of Bill's article, the reasoning is much more down to earth with numerous facts about companies, projects, standards, and markets.

The INDICARE interview with *Jens Redmer*, at present responsible for Strategic Partner Development for Google Book Search in Europe, reveals that Google is not willing at present to go into a strategic debate about its impact on the publishing industry and how it will develop its line of services. The profile of Google Book Search as a book discovery mechanism is underlined, while the potential of services rendering content directly on the Internet is anathema: "Google Book Search is a means for helping users discover books, not to read them online and/ or download them. We will neither put Libraries nor Publishers out of business" (Jens Redmer). What becomes very clear in the interview, however, is that Google Book Search has established sophisticated technical and organisational protection measures to cope with the different demands of its partner libraries and publishers. It does not call them DRM, because "Google Book Search is a book discovery program, not a book reading program. For this, we rather need access limitation mechanisms than DRM mechanisms" (Redmer). That's right. But if we look at the relations between any publisher and Google we see B2B DRM at work: publishers define, i.e. restrict, what Google may do with their content, and these restrictions are implemented by Google defining the usage possibilities/restrictions for consumers.

Monitoring progress of European policy on cross-border licensing for online music

In this issue *Margreet Groenenboom* follows up what she already started in the September issue of the INDICARE Monitor, namely to monitor and analyse EC policy aimed to improve the cross-border licensing for online music services. The basic idea is to come up with EU-wide copyright licenses. Appropriate policy making has already gone through (at least) six steps so far:

- April 2004: The Commission adopts a Communication on the management of copyright and related rights in the Internal Market, i.e. COM (2004) 261 final. Chapter III of this Communication touches upon collective rights management. The Commission indicates that a legislative initiative in this field is required.
- April 2004 – June 2004: A stakeholder consultation takes place with respect to this Communication and collective rights management in particular with 107 stakeholder statements as response.
- July 2005: Publication of a Commission staff working paper: "Study on a community initiative on the cross-border collective management of copyright", which is analysed in the September issue of the INDICARE Monitor.
- July 2005: A stakeholder consultation takes place with respect to the "Study" with 85 stakeholder statements in response.
- October 2005 (11.10.2005): Impact assessment on reforming cross-border collective management of copyright and related rights for legitimate online music services
- October 2005 (21.10.2005): Commission Recommendation of 18 May 2005 on collective cross-border management of copyright and related rights for legitimate online music services

The last two documents are discussed in this issue.

With respect to DRM, the EC expects that rightholders will take into account DRM solutions offered by Collective Rights Managers to protect and monitor their rights in the most efficient way. But as Margreet points out this presumes that "all rightholders favour the use of DRM", which can not be taken for granted as e.g. public statements of artists rejecting DRM systems show. To offer DRMS is not an asset *per se*.

On the other hand the article demonstrates nicely a demand for B2B DRM systems as a prerequisite to manage rights European wide. For example the idea put forward by the Commission that rightholders should be allowed to withdraw licensed rights from a Collective Rights Manager at any time is

hardly realistic without an up-to-date mechanism making transparent and instantly available the information on who is represented by which Collective Rights Managers for which rights.

Conference report

Kristóf Kerényi reports about the ACM's fifth workshop on DRM. He reported last year on the previous workshop, so he is able to compare and analyse trends. One surprising trend he found is that aspects of consumer acceptability are now also acknowledged by technical DRM experts and played a role during the conference. Interesting in this respect was the contribution of *Alapan Arnab* (University of Cape Town), who does not believe in the implementation of "fair use" in DRM systems, and therefore looks for improvements targeting "fairer use". *Rei Safavi-Naini* (University of Wollongong, Australia), also dealt with fair use. Based on her own empirical research she stressed the importance of the social context of music and new media consumption and existing social practices. Acknowledging social practice, DRM systems should strive to enable sharing and exploring new music, a strategy which at the end of the day would also lead to business opportunities. *Andrew Moss*, presented Microsoft's view highlighting consumer acceptability of DRM systems. The challenge today would not be technology but privacy, accessibility, ease of use, interoperability and device-to-device availability. Of course there were more technical presentations, which are all addressed in Kristóf's conference report.

Review of a research paper

In the last article of this issue I review a journal article which investigates the changing boundaries and interrelations of information markets and the public domain. More precisely, *Ursula Holtgrewe* explores the different intellectual property regimes in the music sector and scientific publishing, and provides a picture of the patchwork of for-profit and non-profit activities in these fields. Her ambition is to challenge the "essentialists" who opt for either the market or the public domain, and to overcome what she calls "digital neo-Marxism". Her approach is taken from sociology of knowledge and aims to focus on different levels of knowledge use and interchange. The article is just a preliminary piece of a broader study. What makes this research interesting for INDICARE is the intention to find a third pragmatic route between "essentialist" positions, and to base judgements and recommendations on observations of real world interactions and interchanges.

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 25/11/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=158

Intrusive DRM

The cases of Sony BMG, StarForce and Microsoft

By: Philipp Bohn, Berlecon Research, Berlin, Germany

Abstract: Recently, DRM has attracted broader public attention. The debate was triggered by the news that Sony BMG released selected CDs with copy protection that installed a rootkit affecting the owner's operating system. However, this was not the first time content providers had decided to employ invasive copy protection systems. These cases show that companies employing DRM systems with deep impact do so at the cost of their consumers' interests.

Keywords: news analysis – consumer expectations, privacy, DRMS, technical protection measures, trusted computing, DRM users

Introduction

Mark Russinovich, an independent Windows security researcher, stirred up the blogosphere's attention with an entry in his blog on October 31 (Russinovich 2005), which then diffused into mainstream media. Testing a rootkit revealer he had developed, the program identified some cloaked files of unclear origin. Digging a little deeper, he found that they were installed along with a driver bundled into an audio CD he had purchased earlier. These drivers are employed by record companies in order to play a music CD on a CD-Rom drive and enable "sterile burning" (consumers can make a limited number of copies, which in turn cannot be duplicated again). A rootkit is a set of software that helps an intruder gain access to a computer system.

However, this was not the first time that invasive DRM has been employed, but this time it did not go undetected by the broader public. The amount of attention contradicts the content industry's argument that most users are not aware of and accept DRM. In fact, some 230 consumers posted negative product reviews on Amazon for the CD that sparked the turmoil (cf. Sources).

DRM technology like this directly affects a computers' operating system, disables access to other applications and allegedly exposes the user to security risks. This is the case with Sony BMG's rootkit and StarForce, a copy protection system for video game CDs. Another scenario where the consumer's interests might be considerably affected is the case of Microsoft's DRM licence system. This might also be an issue with alternative DRM systems, such as Apple's FairPlay.

This article discusses these three cases and evaluates the impact they might have on user experience and their attitude towards deep impact DRM and the companies employing it.

The Sony BMG rootkit case

This case has already been outlined in the introduction. In this chapter we go into some detail concerning risks and corporate behaviour in order to highlight some recurring patterns when deep impact DRMS are employed.

Intrusive DRMS create unnoticed security risks

An IT security expert detected the files when testing a rootkit revealer. For the average user, they would remain invisible. Some observers argue that this might pose a security risk to the user, as hackers might try to sneak in malicious code that would hide using the syntax of Sony BMG's rootkit.

On an Internet forum where hackers of the online game World of Warcraft exchange news and ideas, one member rhapsodizes: "For only $14.99 [the price of the CD] you get a well done rootkit" (cf. WOWSharp 2005). Reportedly, a trojan is also exploiting this security leak (cf. SecurityFocus 2005) and a security researcher estimated that about half a million networks have been infected with the files (Norton 2005).

Implementation on operating system level
While "sterile burning" players like those employed by Sony BMG and others are well known, the new thing is that files were installed on the operating system level. While DRM usually tries to control what the consumer does with the content carrier (i.e. number of burns, etc.), these DRM systems directly manipulate the kernel, the operating system's core. The kernel controls access to a PC's hardware and various processes. They supposedly scan for activity indicating attempts of piracy. This consumes resources and power in the process.

Intrusive DRMS overstretch the boundaries of any EULA
Similar to the StarForce representative (see below), a Sony BMG spokesperson implies that by accepting the EULA (EULA is short for "End User License Agreement"), the user agrees to have the rootkit installed on the PC as part of the copy protection system (McMillan 2005).

However, given that some consumers buy a larger number of CDs and install plenty of programs, they can hardly be expected to read through and understand each EULA. And there probably has to be a point where content providers cannot cover everything that is in their interest by a EULA.

In many cases the customer is not informed about detailed specifications of the copy protection system before the purchase. And after reading the EULA, and even if the documents were transparent enough, it would very probably be too late to return the CD and ask for a refund.

Intrusive DRMS are hard to uninstall
After uninstalling the player software, said rootkit files remain on the computer. Manual removal by the expert resulted in temporary loss of the CD-Rom drive. Even the patch offered by Sony BMG originally did not remove the files, but only made them visible.

When accepting the EULA consumers allegedly agree to have the copy protection installed, the companies should assume that they want it removed when agreeing to receive and run a patch. But that is not the case.

Companies hesitatingly admit misconduct
According to the developer of the DRM system, British company First4Internet, "this is old news" (Whipp 2005), as the system had already been employed for a while. So the question remains why action is taken only now, if this is old news. "Consumers, for eight months, have been using these discs with positive feedback. When the issue arose, we addressed it quickly", says *Mathew Gilliat-Smith*, First4Internet's CEO (Pogue 2005). That might probably be a bit too late.

As a result of the debate, Sony BMG finally offered a patch that people had to apply for by filling out a form on the company's website, being asked to submit information such as the point of purchase, the album title and a valid email address. Only from November 10, the company offered a link for direct download of a patch revealing and removing the files. The company eventually decided to pull the discs from the market (Borland 2005a). It would have been an acknowledgement of the inconvenience actually or potentially caused by these measures to do so right away.

In an interview on American national radio Sony BMG's director for digital business, *Thomas Hesse*, notoriously said: "Most people, I think, don't even know what a rootkit is, so why should they care about it?" (Orlowski 2005). Although this statement might be partially attributed to situational distress, it reveals a somewhat frightening lack of respect for the customer.

StarForce

A similar pattern could already have been detected in an earlier case. StarForce is an encryption and activation technology for CD, CD-R and DVD. It is developed by StarForce Technologies and is primarily used to protect electronic games. Basically, what this system does is to deactivate tools that can potentially be used for illegitimate burning of discs, such as Nero Burning or CloneCD. These are reactivated when the user has finished playing the game. In this way, StarForce tries to dictate if or when certain applications can be used.

However, there have been reports on private sites indicating permanent loss of burning software purchased by the user (cf. Parsons 2004). One could argue that this puts every paying customer under the general suspicion of software piracy.

Although it seems evident that customers would not agree to have parts of their property disabled (if only temporarily), one company representative states that "our product is licensed to our customers and becomes part of their product, so the user by accepting the terms [of the EULA] is giving approval" (Wojnarowicz 2004). With DRM getting more invasive, it is time to think about how far-reaching EULAs can be and if the customer's acceptance reveals his actual consent. After all, he has to accept in order to access the content. But when he learns about the EULA's details, it is often too late to return the product.

Confronted with problems customers had reported, the representative replied: "Now that we hear the dissatisfaction about it, we have taken steps to fix it" (Wojnarowicz 2004). It appears to be the tactic to see what is possible and if someone notices, to withdraw due to public pressure.

Microsoft DRM

One of Microsoft's support pages describes the symptoms of the problem I want to discuss in the following: "The Windows Media Digital Rights Management system may not work if you make changes to your computer hardware. You may not be able to play protected content. Protected content includes content such as songs that you have bought and downloaded from an online store" (cf. Microsoft 2004). The reason for this is that users have to authenticate the computers they want to use to play the music they have purchased. So while this prevents the user from illegally swapping files, it may also prevent the user from swapping hardware components, as legitimately purchased property might become inaccessible. This specifically includes crucial components such as the central processing unit or motherboard.

If the consumer is confronted with these problems, Microsoft suggests restoring the PC to its original settings. In case this does not help, a lengthy step-by-step guide is offered to resolve the problem. While this is unnerving for the tech-savvy user, it seems impossible for the average consumer (keep in mind that a lot of people consider programming a VCR too complicated).

But even if the user manages to go through the processes of resetting the computer, back-up the licenses and all the other steps, there still is a chance that purchased files are lost forever. A situation that does not seem to be too far-fetched: "If you cannot back up your license for a particular file, you cannot restore that license after you change your hardware component. If you cannot restore a license, you cannot play the protected file. For more information, visit the Web site of the license issuer to determine whether they support the Backup and Restore feature of Windows Media DRM" (cf. Microsoft 2004).

This practically means that the user has to backup all DRM licenses and if this is not possible, legitimately purchased files might be lost, unless there is support from the distributor. In case there is more than one distributor, things can get even more complicated. Thus, Microsoft's DRM licensing system and authentication policy can make the replacement of hardware an annoying task, probably resulting in the loss of content.

Bottom line

Any invasion by DRM technology that goes beyond the purpose of DRM is at least questionable and should be made more transparent. Furthermore, the companies' reactions failed to show their unconditional willingness to serve the paying consumers' interest. They should keep in mind that they own the music, not their customers' computer.

Sources

- Amazon (2005): http://www.amazon.com/exec/obidos/tg/detail/-/B00092ZM02/qid=1132065594/sr=8-1/ref=pd_bbs_1/104-6037731-7948748?v=glance&s=music&n=507846

- Borland, John (2005a): Sony recalls ´risky´ rootkit CDs. http://news.com.com/2102-7349_3-5954154.html?tag=st.util.print
- Borland, John (2005b): Sony sailing past rootkit controversy. http://news.zdnet.com/2102-9595_22-5965243.html?tag=printthis
- McMillan, Robert (2005): Sony ships sneaky DRM software. http://www.pcworld.com/resource/printable/article/0,aid,123362,00.asp
- Microsoft (2004): The Windows media digital rights management system may not work if your computer hardware changes. http://support.microsoft.com/?kbid=891664
- Norton, Quinn (2005): Sony numbers add up to trouble. http://www.wired.com/news/print/0,1294,69573,00.html
- Orlowski, Andrew (2005): Sony digital boss – rootkit ignorance is bliss. http://www.theregister.co.uk/2005/11/09/sony_drm_who_cares/
- Parsons, Steve (2004): Steve's picks. http://www.joystiq.com/entry/1234000477025364/
- Pogue, David (2005): Sony BMG's copy-protecting watchdog. http://www.nytimes.com/2005/11/09/technology/circuits/09POGUE-EMAIL.html?ei=5088&en=b02a0bc0b7f5dd7f&ex=1289278800&partner=rssnyt&emc=rss&pagewanted=print
- Russinovich, Mark (2005): Sony, rootkits and digital rights management gone too far. http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html
- SecurityFocus (2005): Sony BMG faces digital rights siege. http://www.theregister.co.uk/2005/11/11/secfocus_sony_analysis/print.html
- Whipp, Matt (2005): Sony DRM company declares rootkit issue ´old news´ and offers fix. http://www.pcpro.co.uk/news/79491/sony-drm-company-declares-the-issue-old-news.html
- Wojnarowicz, Jakob (2004): StarForce interview and piracy discussion. http://www.firingsquad.com/features/starforce_interview/page2.asp
- WOWSharp (2005): Lowcost superb RING0 rootkit developed (payed) by Sony BMG. http://www.wowsharp.net/forums/viewtopic.php?t=7251

About the author: After having graduated from University of Mannheim (Business Administration), *Philipp Bohn* has joined Berlecon Research as Junior Analyst. He is a member of the INDICARE-team. Contact: pb@berlecon.de

Status: first posted 24/11/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=155

Rights management and the revolution in e-publishing

By: Bill Rosenblatt, President, GiantSteps Media Technology Strategies, New York, USA

Abstract: Google Book Search and the handful of developments in its aftermath are ushering in the next wave of digital publishing. Discoverability and rendering of copyrighted works on the Internet add up to the most disruptive force to publishers' lines of business at least since the emergence of desktop publishing in the 1980s. Digital rights management plays a crucial role in this e-publishing revolution. In this article, we outline the big changes in online publishing today, and we discuss the role that DRM plays in new online content distribution, discovery, and retail initiatives, and how it should play a role in the future.

Keywords: policy analysis, economic analysis – business models, e-books, Google, publishing

The end of growth in eBooks

Many types of DRM technologies were offered to the publishing industry over the past decade, but few of them caught on. For the past six years or so, DRM has largely meant only one thing in the book-publishing world: eBooks. The eBook market emerged and rapidly consolidated during the Internet bubble of 1999-2000, and never really measured up to the hype that surrounded it (cf. Bohn 2005).

Two signposts for the end of growth in the eBook market appeared recently: first, in November 2004, Adobe quietly announced plans to withdraw its market-leading eBook DRM packaging software (Adobe Content Server) from the market and shift its focus to corporate document security (cf. Rosenblatt 2004); second, the trade association Open eBook Forum (OeBF) changed its name to the International Digital Publishing Forum in April 2005.

The usual reason given for eBooks' lack of success is that most consumers don't like reading books on PCs or dedicated hardware devices such as those from Gemstar and Franklin. But an equally important reason is that publishers only really accepted eBooks as digital facsimiles of print books that were cheaper to manufacture and distribute. Publishers did little to explore the potential of eBooks to implement new business models or new ways of distributing content – not even in markets that seemed especially promising, such as professional and higher education publishing.

The lack of innovation around eBooks can be largely attributed to publishers' reluctance to disrupt their existing supply chains, which, after all, they have cultivated carefully over a period of centuries.

Google Book Search

Google's Google Book Search program, which emerged in July 2005 (and which was called Google Print until mid-November), represents the biggest threat to those supply chains in a long time. Google has been scanning, digitizing, and indexing tens of thousands of print books, mostly borrowed from prominent university libraries, and making their texts searchable online.

The Association of American Publishers (AAP) organized a lawsuit against Google in October 2005, on behalf of five major US-based book publishers, alleging that Google infringed copyright when it scanned and indexed books without publishers' permission (cf. AAP 2005). But that allegation was more like a subterfuge: supply chain concerns are the biggest reason for the publishing industry's concerns about Google.

The truth is that Internet search engines like those of Google, Yahoo, and MSN have the potential to radically change the business landscape for book content, because they capture consumers' interest at the primary point of *discoverability* for content online. A search engine has the power to expose content as the result of a user's Internet search, direct her to any other resource on the Internet to find the full content… and potentially make money on the referral.

In the publishers' lawsuit (and a similar one brought by the Authors Guild; (cf. Authors Guild 2005), Google is arguing that its use of the print books is legal according to US copyright law (17 U.S.C. 107), which judges "fair use" of content based on four principles. One of those principles is the effect that the use has on the market for the content; Google claims that because it is helping more consumers purchase more content, its effect on the market is positive for publishers.

However, another of the four principles is the purpose and character of the use, including whether such use is of commercial nature. In addition to the revenue that Google currently garners from ads that it displays alongside book content in search results, the potential number of content transactions from which Google could directly benefit financially is staggering.

To put the potential impact into some perspective: the technology that may currently be the largest source of online referrals to copyrighted text works is Amazon's affiliate marketing program, Amazon Associates. Amazon Associates' websites contain specially encoded links that lead users to purchase pages on Amazon; if the user makes the purchase, the Associate earns a commission. Although there are over a million Amazon Associates, the impact of Google's ability to lead consumers to copyrighted material has the potential to dwarf that of the Amazon Associates program: bear in mind that *any* Google search can lead a user to book content, whereas users must click on special URLs to find book content through Amazon Associates.

DRM and the discoverability paradox

Discoverability of copyrighted works online has been a stumbling block to the growth of the market for online content. It is a paradox: many copyrighted works – those generally judged to be the most valuable – are the hardest to find on the Internet. Publishers are concerned about piracy of their valuable works (as opposed, say, to copyrighted works judged less valuable, such as ephemeral news stories), so they don't expose them online, which means that users of search engines can only find them through more limited means, such as summaries, abstracts, and metadata.

DRM provides a way out of this paradox – and not just in theory. Perhaps the cleverest application of DRM to making copyrighted works discoverable was a technology called eLuminator, which appeared around 1999. ELuminator was the product of MediaDNA, a DRM startup that originated in Sweden and subsequently moved to the United States.

ELuminator worked by extracting all of the nontrivial words from a document – a typical step in search engines' text indexing techniques – and placing them on a web page as invisible meta-tags. Search engines would then index that page, so that users searching for words included in the text would find the page in search results. The visible portion of the page would contain an offer to purchase a version of the document that was packaged (encrypted) with MediaDNA's proprietary DRM.

In other words, eLuminator was a fancy, automated version of what we now call search engine optimization (SEO): the art and science of tweaking web pages so that the major search engines are more likely to give them more favourable search result rankings. Unfortunately, eLuminator did not catch on with publishers beyond a handful of pilot projects. MediaDNA ceased operations, sold eLuminator to Inceptor (an SEO technology company), and sold its core DRM technology to Macrovision – all in late 2001.

With Google Book Search, Google is, in a way, taking the eLuminator concept to the next level. It indexes the text of copyrighted works and makes them available for viewing, but only a few lines at a time – just enough to provide context around search results. This is really just a form of access control, i.e., DRM.

Once a user sees book text in Google search results, Google could then offer to sell the user a DRM-protected document itself; but instead – at least for now – it provides links to other websites, such as Amazon, Barnes & Noble, BookSense, and publishers' own websites, for purchase of physical products. (It could just as easily refer users to purchase opportunities for other versions of the content, such as eBooks at eReader.com or OverDrive, or audiobooks at Audible.com.)

More recently, Google has been holding discussions with book publishers about supporting a weekly rental model, somewhat like a cross between a public library and an online video-rental service like MovieLink. The discussions are very preliminary at this point, but one thing is for sure: Google will need to adopt full-blown DRM technology in order to make that model work. Although Adobe's Content Server technology might be available for acquisition, one suspects that, given its history, Google will design its own.

Amazon and the Open Content Alliance

Amazon itself announced plans in November 2005 to take the concept of online rendering a step further (cf. Amazon.com 2005). Amazon already offers "Search Inside the Book," a feature that makes a small number of pages in books available for online viewing in a streaming-style page rendering format that inherently deters piracy. It intends to extend this in two ways: Amazon Pages, which will enable users to purchase content by the page rather than by the book, and Amazon Upgrade, which will enable purchasers of print books to view their contents online for an additional fee.

Both of these programs will build on the technology from Search Inside the Book. It is unclear whether the increased amount of digitized text that Amazon will create as a result of these new programs will enable it to make that text discoverable by search engines.

It is worth noting that Amazon quietly purchased a French eBook technology company

called Mobipocket in March 2005. Mobipocket's eBook platform for a variety of handheld devices is fairly popular in professional and technical publishing, an analog to eReader's platform for trade eBooks (cf. Rosenblatt 2005a). Amazon has done nothing (publicly) with Mobipocket's technology, which affirms that the future of online publishing is direct Internet rendering rather than downloads to closed devices.

An organization called the Open Content Alliance (OCA) formed in October 2005, shortly before the publishers filed their suit against Google. Yahoo and Internet Archive were the co-founders; now the membership also includes Microsoft's MSN, O'Reilly Media (a publisher of IT-related technical works and prominent open source advocate), and several archives and libraries. The intent of OCA is similar to Google Book Search, with one important difference: while Google Book Search has had an "opt out" policy toward publishers (i.e., publishers must notify Google if they do *not* wish their books to be scanned), OCA is "opt in" (publishers must give the OCA permission upfront to scan and digitize their books).

It is possible to view all of these initiatives as implementations of DRM or DRM-like mechanisms that are built for specific, narrow purposes. Google Book Search indexes the full text of books, controls access to the text by only exposing it a few sentences at a time, and facilitates commerce in rights to the text by passing users along to others via links.

Amazon's Search Inside the Book technology, meanwhile, controls access to text by only exposing it a page at a time. A precedent for this is ebrary, an online library service that was founded in 1999 with backing from Adobe and three major book publishers, and that now serves both schools and public libraries; ebrary lets users query large repositories of book content and view text, through a browser interface, a page at a time.

Amazon Pages, using the Search Inside the Book technology, facilitates commerce in rights internally by allowing users to purchase access to ranges of pages. Time will tell what kinds of mechanisms Yahoo, MSN, and other OCA members will use to provide controlled access to copyrighted content.

Publishers are effectively at the mercy of these narrow technologies and thus of the business models that they enable. Of course, it works both ways: these technology companies cannot offer online content without publishers' blessings. In Amazon's case, Amazon Pages arose out of a decision by Random House – a division of Bertelsmann AG and the world's largest trade publisher – to support page-at-a-time access rights via micropayments.

Publishers' responses

Internet-based discoverability and content display can be powerful forces for publishers if they harness them appropriately rather than simply letting technology companies take the reins. Two initiatives in Germany, announced during this year's Frankfurter Buchmesse (Frankfurt Book Fair) in October, represent attempts to do this. One comes from the publisher Verlagsgruppe Georg von Holtzbrinck; the other from the Börsenverein des Deutschen Buchhandels (German booksellers' trade association).

Holtzbrinck is developing a system it calls BookStore, which it will use for its own publishers' content but also offer to other publishers. BookStore will be an online text repository with its own e-commerce capabilities as well as the ability to make text available to search engines for indexing. BookStore is being developed by MPS Technologies, a subsidiary of Holtzbrinck's Macmillan unit based in the UK and India (cf. MPS Technologies 2005).

The Börsenverein is working on something similar, which it calls "Volltextsuche Online" (Full Text Search Online): a text repository that publishers can use for their own material and that enables searching across the repositories of all publishers that use the system. Search engines like Google and Yahoo would be able to search those repositories directly instead of scanning content into their own infrastructure, and the Börsenverein is in talks with search companies about this type of arrangement (cf. Börsenverein 2005).

The main difference between Holtzbrinck's BookStore and the Börsenverein's Volltextsuche Online is that the latter is oriented toward "federating" search for book content, so that companies like Google and Yahoo do not end up with monolithic collections of copyrighted material. BookStore is really more like an incremental improvement on online eBook retail system providers such as OverDrive, the improvement mainly being the system's ability to release full text to search engines for discoverability purposes, instead of just making abstracts and metadata available (as Amazon and its ilk do today).

It's about the rights

Unfortunately, both of these proposals miss the point. Once copyrighted content exists *somewhere* on the Internet, it's no longer about the content – it's about the rights. If publishers want to maintain control over their own rights and supply chains in the Internet age, then they will need to take control of their *rights* and how they make them available to distributors and retailers like Google, Amazon, Yahoo, and MSN. Then the content can be served up from wherever it is.

Right now, publishers grant or deny certain rights to online distributors in ad-hoc ways. In the case of Amazon and its new initiatives, the rights are bounded and well understood. But in the cases of Google Book Search and the OCA, the rights effectively pass out of publishers' control once they give the service provider the right to scan and index the content; their only recourse is contractual.

At this point, Google can simply provide links to other sites that presumably already have rights to sell publishers' product in pre-existing forms. The true power and flexibility of the Internet emerge once publishers can supply companies like Google with rights to digital content, which can be realized through interfaces to all kinds of devices and services.

In effect, this means that publishers should be supplying rights descriptions to online distributors in forms that they can handle – i.e., in machine-readable form. The publishing industry (at least in the US) started to look at this issue in the context of bundling rights with eBooks. In 2003, the OeBF Rights and Rules Working Group (RRWG) defined a rights expression language (REL) standard (cf. IDPF 2003) based on the ISO standard MPEG REL (cf. sources). The UK-based publishing industry e-commerce standards organization EDItEUR has also been working on developing rights-related standards for book content, with library usages particularly in mind.

The MPEG REL is a reasonable starting point, but it is not really designed for this purpose. It is designed to convey descriptions of rights and their attributes (e.g., identities of grantors, payment terms, identities of grantees) to end-users through their hardware devices or software. The language is not intended to automate rights aspects of distributor relationships.

Another standards initiative called the Content Reference Forum (cf. sources) is not only intended to address this particular problem but is also intended to be compatible with (and complementary to) MPEG REL. The CRF, which arose primarily out of the music industry, was created to automate rights processing aspects of multi-tiered content distribution networks. Its most important work product has been the Contract Expression Language (CEL), a machine-readable language that expresses distribution relationships along with rights, obligations, financial terms, and so on. Unfortunately, neither the OeBF RRWG nor the CRF have seen much activity since the end of 2003.

The publishing industry could revisit standards initiatives like the OeBF MPEG REL extensions, the CRF, and some of those cited in *Brian Green's* recent INDICARE article on EDItEUR initiatives (Green 2005). Holtzbrinck, for example, could then build standard rights and distribution terms expressions into its BookStore system.

There is an important precedent for this type of standards-based supply chain automation in the publishing industry: the ONIX standard for book product metadata (cf. sources), which many publishers use to feed product information to Amazon and other distributors and retailers, and which has substantially improved the efficiency of this process.

ONIX contains fields for such things as book identifiers (e.g., ISBN, UPC, DOI), product metadata (e.g., price, minimum order quantity), physical characteristics (e.g., size, weight), and descriptions of content. The AAP steered the development of ONIX, and it is maintained by EDItEUR along with the Book Industry Study Group in the US. There is also a version of ONIX for serials content, such as academic journals.

At the same time, just defining standards for communicating rights information to online distributors is not enough. Publishers must be able to define and manage those rights for themselves first, so that they can express them mechanically in a REL or similar technology. Yet few publishers have viable internal databases of the rights that they are entitled (e.g., by contract) to offer; solving this problem can involve large-scale system development, process rationalization, and (in many cases) integration with legacy systems. Publishers must also think seriously about what rights they are willing to offer to online distributors, of the ones that they are able to offer. Random House's decision to offer per-page rights through Amazon is only a small step in that direction.

Bottom line

Throughout the development of the Internet, publishers have had various opportunities to take control and make the most of this hugely impactful new medium as it moves from physical commerce facilitator to content distribution and rendering medium. Developments like Google Book Search show that technology companies have the potential to force dramatic changes to publishers' business models and supply chains. Publishers must realize that once content is out there on the Internet, control over rights is the key to control over their industry's future. If they do not act soon, then Internet technology companies will take over their supply chains, they will be marginalized into lesser relevance in the content world, or both.

Sources

- AAP (2005): Press release on publishers' lawsuit against Google; http://www.publishers.org/press/releases.cfm?PressReleaseArticleID=292
- Amazon.com (2005): Press release on new digital text initiatives; http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=778248&highlight=
- Authors Guild (2005): Press release on authors' lawsuit against Google; http://www.authorsguild.org/news/sues_google_citing.htm
- Bohn, Philipp: eBooks – The stony road to success and the role of DRM. INDICARE Monitor, Vol. 2, No 5, July 2005; http://www.indicare.org/tiki-read_article.php?articleId=127
- Börsenverein des Deutschen Buchhandels (2005): Press release on Volltextsuche Online; http://www.boersenverein.de/de/98462?skip_val=&list_id=64641&jahr=&aktuell=yes
- Content Reference Forum: http://www.crforum.org/
- Green, Brian: Helping libraries manage digital rights. INDICARE Monitor, Vol. 2, No 7, September 2005; http://www.indicare.org/tiki-read_article.php?articleId=140
- IDPF Rights and Rules Working Group (2003): Coordinated Requirements; http://www.idpf.org/specifications/rrwgcoordinated.htm
- MPEG REL (ISO/IEC 21000-5:2004); http://www.iso.ch/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=21000-5
- MPS Technologies (2005): Press release on Holtzbrinck's BookStore; http://www.mpstechnologies.com/pdfs/19.10.05.pdf
- ONIX: http://www.editeur.org/onix.html
- Open Content Alliance: http://www.opencontentalliance.org/
- Rosenblatt, Bill (2004): Public libraries offer new digital content formats. The Seybold Report, Vol. 3, No. 24, March 29, 2004, pp. 15-19; http://www.seyboldreports.com/TSR/subs/0324/digital.html
- Rosenblatt, Bill (2005a): Amazon acquires Mobipocket. DRM Watch, April 21, 2005; http://www.drmwatch.com/drmtech/article.php/3499386
- Rosenblatt, Bill (2005b): Publishers seek alternatives to Google Print. DRM Watch, October 27, 2005, http://www.drmwatch.com/legal/article.php/3559606

About the author: *Bill Rosenblatt* is president of GiantSteps Media Technology Strategies, a consultancy based in New York, USA that focuses on digital content technology issues for content providers and technology vendors. He is editor of the newsletter DRM Watch (http://www.drmwatch.com) and author of *Digital Rights Management: Business and Technology* (John Wiley & Sons, 2001).

Status: first posted 21/11/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=152

Google Book Search

Fostering public access in a controlled way

By: Jens Redmer, Google Book Search Europe, Hamburg, Germany

INDICARE-Interview by Knud Böhle, ITAS, Karlsruhe, Germany with Jens Redmer, Google Book Search Europe. The interview makes the essence of Google Book Search clear: an innovative and powerful Online Public Access Catalogue integrated into Google's overall index and search service for the Internet. Due to the focus of the INDICARE Monitor questions centre on content protection, usage limitations, and copyright.

Keywords: interview – access control, business models, copyright law, Google, libraries, public domain, publishing, technical protection measures

About Jens Redmer: *Jens Redmer, born 1967, studied computer science and medicine at Kiel University, Germany. From 1995 until 1998, he directed various projects in the fields of interactive media within the Axel Springer Publishing Group's Strategic Planning Department. Last position at Springer was regional MD for a local internet service provider, a Bertelsmann/ Springer/ WAZ joint venture. From 1998 until 2001, he directed Business Development for ricardo.de, a pan-European internet auction site as a member of the Board. Further stations of his development include AOL Germany, where Jens directed Premium/ Paid Services from 2001-2004, and Endemol TV Productions in Amsterdam/ The Netherlands and Cologne, Germany, 2004-2005. Here Mr Redmer directed Endemol's multimedia department. At present he is responsible for the Strategic Partner Development for Google Book Search in Europe.*

INDICARE: Mr. Redmer, there are gigabytes of articles about Google Print recently renamed Google Book Search (Grant 2005) and information by Google itself (cf. sources). Nevertheless, let's start with some up to date figures about the *Google Book Search Library Project* and the *Google Book Search Publisher Program* to set the scene: How many books have you scanned already? How many books are available online via Google Book Search? How many libraries are actively participating in Google Book Search for Libraries? As there are news (cf. e.g. Charny 2005) that you are giving more attention to the European region than before; who are the European libraries and publishers currently participating?

J. Redmer: We have experienced a tremendous interest in our program so far. Up until today, thousands of publishers have successfully joined Google Book Search. Let me point out that virtually every major US and UK publisher is an active member of the Google Book Search Program. Our commitment to create a truly international product has just been underlined by our recent launch of Google Book Search in many more languages in European countries, including France, Italy, Germany, Spain, and the Netherlands. In the Library program, we currently work with 5 leading libraries, 4 of which are based in the US (Universities of Stanford, Harvard, Michigan, NY Public Library) plus our first European Library partner, the University of Oxford. We continue to explore

further partnerships and expect to cooperate with additional Libraries soon. Google is international, so language diversity is key.

INDICARE: As INDICARE is especially interested in DRM from the consumers' point of view, could you please split the number of titles available in those already in the public domain, those from libraries still under copyright, and those made available by publishers?

J. Redmer: While I cannot disclose the actual numbers within our Publisher and Library Programs, let me explain that right now, most of our books come from the Google Book Search Publisher Program, a program that lets book publishers of all sizes have their book content included in Google's main search results. Publishers send us their books and we digitally scan them and add their content to our search results – all for free. Through our partnerships with well-known libraries, through the Google Book Search Library Project, over time your Google search results should start to show more books from these collections as well.

INDICARE: Please allow me to insist on figures, although I know Google is somehow reluctant to communicate them. The order of magnitude of books covered by the *Google Book Search Library Project* and the *Google Book Search Publisher Program* respectively should be no secret.

J. Redmer: These numbers are big. Really big. But, unfortunately, I cannot share the actual number with you. You will get a good indication of the magnitude of the books covered within the Google Book Search by trying it out yourself for a set of search requests by navigating to http://books.google.com.

INDICARE: There are different usage restrictions for each of these types of sources, as explained roughly in the "Google Book Search Help Center" (cf. sources). Could you explain in technical terms how content protection works in Google Book Search, and what is even more interesting, the reason why exactly you have chosen the different sets of usage restrictions.

J. Redmer: Google carefully respects rights of all copyright owners, this is why we restrict usage of the books discoverable on Google Book Search. Google hosts all material on our secure servers. We disable the print, cut, copy, and save functionality on all pages displaying book content, in order to protect the material. Of course, also no downloading is possible. In addition, the publishers can choose how much of a book a user will be able to view over a 30 day period, from 20% to 100%. Adding to these user-focused restrictions, there are also page-level restrictions. Portions of the book will be available to all identifiable users (using the cookie technology), but those users wanting to browse additional pages must additionally sign in with their Google Account to view the full pages. They will still be restricted to the percentage of the book a publisher chooses to make available. At all times, only a part of the book is online since Google makes a significant portion of a book invisible to all users.

INDICARE: Google's content protection policy may seem to some already exaggerated, for example I wonder why you don't offer a download function or at least a print function for books 100 % out of copyright.

J. Redmer: Again: Google Book Search is a means for helping users discover books, not to read them online and/ or download them. We will neither put Libraries nor Publishers out of business. Because of this, users who want to read the whole book can use the "Buy the Book" links to purchase it. Users can also click through to the publisher's website where there may be a digital version available. If the book that a user discovered is no longer in print, we link users to libraries where they can find the book to access the book in physical form. Google Book Search supports all parties: It drives publisher sales by leading our users to book retailers including the publisher's website, and it also helps libraries fulfil their mission better by leading our users into libraries.

INDICARE: I see; in essence Google Book Search is a sophisticated "Online Public Access Catalogue" (OPAC). Last year Electronic Frontier Foundation's Cory Doctorow

indicated that *Seth Schoen* (EFF's so called staff technologist) had found "some avenues toward breaking" Google Book Search's DRM (Doctorow 2004), and more recently *Greg Duffy* (alias Isometrick) claimed to have written a "simple code that can instantly create PDFs of entire books from Google Book Search" (Duffy 2005). Do you believe that these hacking tools really do what they promise? Has Google Book Search already been hacked? Have you done anything meanwhile to repair these security breaches?

J. Redmer: Google is in the focus of users trying to get unauthorised access to our services frequently, independent of the Google Book Search Program. Thus, we are used to identifying inappropriate usage patterns for all of our products. As explained above, we have developed sophisticated and extensive technology that strictly limits the access for a single user. Please also bear in mind that at no time, a full book is online since we make a significant percentage invisible to all users at all times. Also, book pages visible within Google Book Search are shown at a very low resolution that is not usable for further processing – high-resolution images are not even connected to the internet. We can identify repetitive usage patterns and react appropriately. Since a book is never online in full, no one is able to view a full book, even with thousands of search requests and multiple machines.

There may be a very small fraction of users trying to circumnavigate access limitations (by the way: that is not "hacking"). Much more importantly, these users are by far outnumbered by thousands, millions of new users that discover – and possibly buy – books that they may not even have been thinking of.

Let me counterask the following questions: Can an offline bookseller guarantee that no-one is reading an entire book on their premises (and not buying it)? Can they guarantee that no-one is taking photos of all those pages of interest to that user, in high resolution, without any limitation? Can a library guarantee that no-one is reading and copying – legally – a full book on their premises? Can a publisher guarantee that one of their books are available on the internet illegally, in full, in high resolution?

Here's our answer: We do not create new risks here, we minimize them. In addition, we constantly add new security features, for example the page-level login requirement recently launched. Google Book Search is not a threat, it is a fantastic opportunity for both authors, publishers, and libraries – and, of course: new readers.

INDICARE: In a way we might say Google Book Search needs DRM technology to be viable?

J. Redmer: Google Book Search is a book discovery program, not a book reading program. For this, we rather need access limitation mechanisms than DRM mechanisms.

INDICARE: Google has been sued by the Authors Guild (Authors Guild 2005), and more recently by the Association of American Publishers (AAP 2005) for copyright infringement (cf. Band 2005a and b for a neutral analysis of the copyright issues). I don't expect statements on these pending law suits, but I would like to ask you what the real foundations of the controversy are. While you are expanding the commons or better, access to them, you pose a threat to commercial publishers' business models – that's more or less what e.g. *Lawrence Lessig* (2005) assumes. One might add that publishers will fear that Google will be able to derive new value-added services from the database of scanned books without revenue sharing with publishers. How do you cope with publisher concerns?

J. Redmer: Let me point out one very important thing here: Google Book Search does not threaten authors' and publishers' business models, it helps drive their businesses. This is very widely misunderstood. Whatever we do is in the interest of both authors and publishers.

We regret that the groups mentioned above chose to sue us over a program that will make millions of books more discoverable to the world – especially since any copyright holder can easily exclude their books from the program, so: no law suit required. What's more, many of Google Book Search's chief

beneficiaries will be authors whose backlist, out of print and lightly marketed new titles will be suggested to countless readers who wouldn't have found them otherwise.

Let's be clear: Google doesn't show even a single page to users who find copyrighted books through this program (unless the copyright holder gives us permission to show more, like in the Publisher Program where we explicitly sign an agreement with publishers). At most we show a brief snippet of text where their search term appears, along with basic bibliographic information and several links to online booksellers and libraries.

The use Google makes is fully consistent with both the history of fair use under copyright law, and also all the principles underlying copyright law itself. Copyright law has always been about ensuring that authors will continue to write books and publishers continue to sell them. By making books easier to find, buy, and borrow from libraries, Google Book Search helps increase the incentives for authors to write and publishers to sell books.

To achieve that goal, we need to make copies of books, but these copies are permitted under copyright law. For those books still under copyright Google is only showing: (1) bibliographic card-catalog-like information and, (2) at most very brief text excerpts. For copyrighted books, full text will not be available, and extensive safeguards to prevent copying and excessive access are in place.

Think of Google Book Search this way: it is very similar to web search. In order to electronically index a webpage, you need to make a copy of it. In order to electronically index a book, we have to make a digital copy of the book. As with web search, the copies we make are used to direct people to the books. Our experience with web search is that many people ask to have their web pages included in our search results and very few ask to be excluded.

INDICARE: Google Book Search, as acknowledged by many, could become a milestone towards a true "docuverse" envisaged by *Ted Nelson* more than 30 years ago. In the words of the National Consumers League (2005) the same vision is present: "If properly constructed and wisely administered, this new venture sets the stage for a quantum leap in consumer access to information". In the light of this great perspective one may however argue that Google's approach is not yet open enough. As researchers from OCLC (cf. Lavoie et al. 2005) estimated, the titles of the five major libraries (Google 5) would just cover a third of the entire record of publications. To be really successful building the new Commons there should be ways to offer a more federated approach, and an approach which leaves more autonomy and ownership with the libraries. How does Google reconcile the public interest in a true docuverse (without artificial proprietary boundaries) with the private company's profit maximising business strategy?

J. Redmer: Thank you for this important question which is easily answered by citing our mission: "To organise all the world's information and make it universally accessible and useful". With Google Book Search, we have just tapped into the vast amount of content that today is not yet accessible online. We will continue to create and improve products to make accessible and useful much more of today's offline content. Allow me to quote our founders: "We are only at the beginning".

INDICARE: Frankly speaking, I would have expected a less easy answer outlining your strategic ideas about co-operation, sharing, federating etc. I can hardly imagine that the Internet population (whatever this may be in social terms) will ever accept a monopolistic gateway regulating access to its record of information…

J. Redmer: Google is constantly aiming at creating even better products to fulfil our mission to organise the world's information and make it universally accessible and useful. As with all products, it is the user who decides if they are helpful and useful. We are very happy with the fact that we are successful with matching user demands with our exiting products, existing and coming.

INDICARE: Thank you very much for this interview.

Sources

- AAP (The Association of American Publishers) (2005): Publishers sue Google over plans to digitize books. Google Print Library Violates Publishers' and Authors' Rights.Press release, 19 October 2005; http://www.publishers.org/press/releases.cfm?PressReleaseArticleID=292
- Authors Guild (2005): Authors Guild Sues Google, Citing "Massive Copyright Infringement". Press release, September 20; http://www.authorsguild.org/news/sues_google_citing.htm
- Band, Jonthan (2005a): The Google Print Library Project: A copyright analysis; http://www.policybandwidth.com/doc/googleprint.pdf
- Band, Jonthan (2005b): The Authors Guild v. The Google Print Library Project.LLRX.com 15.10.2005; http://www.llrx.com/features/googleprint.htm
- Charny, Ben (2005): Google Print goes to Europe. PC Magazine 10.18.05; http://www.pcmag.com/article2/0,1895,1872542,00.asp
- Doctorow; :Cory (2004): HOWTO break Google Print DRM. BoingBoing, Friday, October 8, 2004; http://www.boingboing.net/2004/10/08/howto_break_google_p.html
- Duffy, Greg (alias isometrick) (2005): Hacking Google Print. Kuro5hin 8.3.2005; http://www.kuro5hin.org/story/2005/3/7/95844/59875
- Google Book Search website: http://books.google.com/intl/en/googlebooks/about.html
- Google Book Search website/ FAQ info site: http://books.google.com/
- Google Book Search Help Center: What will users be able to view?; https://print.google.com/support/publisher/bin/answer.py?answer=17853&topic=319
- Grant, Jen (2005): Judging Book Search by its cover. Google Blog 17.11.2005; http://googleblog.blogspot.com/2005/11/judging-book-search-by-its-cover.html
- Lavoie, Brian; Silipigni Connaway, Lynn; Dempsey, Lorcan (2005): Anatomy of aggregate collections. The example of Google Book Search for Libraries. D-Lib Magazine, 11(2005)9; http://www.dlib.org/dlib/september05/lavoie/09lavoie.html
- Lessig, Lawrence (2005): Google sued (22.9.2005); http://www.lessig.org/blog/archives/003140.shtml
- National Consumers League (2005): Letter to the chairmen of the House and Senate Judiciary subcommittees overseeing intellectual property issues; http://www.nclnet.org/news/2005/NCL_Smith.pdf

Status: first posted 23/11/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=153

Commission Recommendation on cross border licensing: Last train boarding now!

By: Margreet Groenenboom, Institute for Information Law, Amsterdam

Abstract: The "Study on the cross-border collective management of copyright" released in July 2005 by the European Commission (EC) was discussed in the INDICARE Monitor of September 2005 (Groenenboom 2005). The present article is a follow up reviewing the EC's subsequent Impact Assessment and the ensuing Recommendation. The article also elaborates on some specific proposals brought forward by stakeholders in their reactions to the Study.

Keywords: review – collecting societies, competition, DRMS, licensing contracts – EU

Introduction

The "Study on a community initiative on the cross-border collective management of copyright" released in July 2005 by the EC aimed to improve the cross-border licensing for online music services (European Commission 2005a). In this Study, the EC proposed three options for the improvement of the current situation:

1. do nothing;
2. suggest ways in which cross-border cooperation between national collective rights managers in the 25 Member States can be improved;

3. give rightholders the additional choice of authorising a collective rights manager for the online use of their musical works across the entire EU.

The EC favours option 3, since first, option 3 enables rightholders to choose the collective rights manager (CRM) they want to join. Secondly, this option enables competition between CRMs, and, as a result, this would lead to the improvement of services offered by CRMs (European Commission 2005b). This competition between CRMs would result in a "survival of the fittest", and, as a consequence, there would be fewer CRMs for online music services to address which would diminish the licensing costs.

Eighty-five stakeholders submitted reactions to the Study to the EC. This article examines the Impact Assessment (European Commission 2005c) conducted by the EC following the reactions submitted, as well as the ensuing Recommendation (European Commission 2005d).

Impact Assessment

The instrument of the Impact Assessment was introduced in 2002 by the EC to improve the quality and coherence of the policy development process for all major initiatives, i.e. those initiatives which are presented in the Annual Policy Strategy or in the Work Programme of the EC (European Commission 2005e). In an Impact Assessment – which should contain certain components – a systematic analysis of the likely impacts of intervention by public authorities can be found. It should be noted that an Impact Assessment is not a substitute for a political decision; however, it might increase transparency, communication and information on the EC's proposals.

In October 2005, the EC released the Impact Assessment on the cross-border licensing of online music services, which contained 7 Chapters:

1. Problem definition;
2. Objectives;
3. Policy options;
4. Analysis of impacts;
5. Assessment and evaluation;
6. Results of stakeholder consultation;
7. Commission proposal and justification.

Chapters 1 to 3 of the Impact Assessment roughly correspond to Chapters 1 to 3 of the Study. Although their titles differ, Chapter 5 of the Impact Assessment (called assessment) generally corresponds to Chapter 5 of the Study (called monitoring). Therefore, this article will focus only on the Chapters of the Impact Assessment relating to the Analysis of impacts (Chapter 4), the Results of the stakeholder consultation (Chapter 6) and the Commission proposal and justification (Chapter 7).

Analysis of impacts (Chapter 4)

In this Chapter, the EC sets out the submissions of the stakeholders per topic, i.e. legal certainty, transparency/governance, culture/creativity, innovation and growth, competition, employment, consumer/prices, impacts outside the EU, consequences for large and medium CRMs, consequences for rightholders and consequences for online music providers. For each topic, the EC concludes by making its own evaluation. All topics gave rise to intense discussion amongst stakeholders, discussion which often centred on the question: who benefits from option 2 or option 3? With respect to this issue, the EC recognises that the basic difference between option 2 and option 3 is that option 3 would introduce competition in the relationship between rightholder and CRM (the rightholders option), while option 2 would introduce competition at the level of commercial users (the commercial user option). If, according to option 3, rightholders would be given the choice which CRM to join, CRMs must ensure their attractiveness to attract rightholders. This means for instance low transaction costs and high royalties. Option 2 would lead CRMs to ensure their attractiveness for commercial users, this means for instance offering a good repertoire and low royalties.

The EC also pays attention to the possible use of DRM by CRMs. The EC expects that rightholders will take into account the DRM solutions applied or imposed by the CRMs to protect and monitor their rights in the most

efficient way. This could have an impact on the development of DRM.

Results of the stakeholder consultation (Chapter 6)

In this Chapter, the EC summarizes per category of stakeholders the favoured options. It is important to note here, that the stakeholder consultation described in Chapter 6 of the Study concerns a prior consultation round, which had been launched on 16 April 2004. Overall, the general opinion of stakeholders in the July 2005 consultation is that indeed something needs to be done, for no stakeholder favours option 1 over option 2 or 3.

Option 2 – suggest ways in which cross-border cooperation between national collective rights managers in the 25 Member States can be improved – is favoured by:

- *Author's societies.* GESAC favours option 2, but stresses that additional safeguards are indicated; first, safeguards against dumping of valuable repertoire by smaller rivals within the network of reciprocal representation agreements and, second, safeguards that enable CRMs to control the price of their own repertoire. These safeguards are needed because GESAC fears that when collecting societies all offer the same (popular) repertoire as a result of implementing option 2, this would result in a downward movement with regard to the amount of royalties being paid to authors. To attract customers, CRMs should offer customers (i.e. online music services) a good price for getting a license. Competition between CRMs for customers would thus lead to lower licensing prices. Lower licensing prices automatically lead to a lower royalty to be paid to authors. With regard to this pricing issue, some very large authors' societies (such as the UK and French societies) are willing to withdraw from reciprocal arrangements with authors' societies that devalue their repertoire by undercutting on the price.
- *Major record companies.* Because they are licensees of authors' rights and thus are amongst the commercial users, they wish to minimise the payment of royalties to be paid to authors' societies. Unlike the author's societies, they favour the downwards pricing movement resulting from competition amongst CRMs to attract customers.
- *Record producer societies.* Because they would like to improve governance and accountability in reciprocal agreements, they favour option 2.
- *Radio broadcasters.* Since they are amongst the commercial users and they aim to serve the market at the lowest possible price, they favour option 2 with an EU wide one stop shop license.
- *Niche European cross-border television channels* (e.g. MTV). MTV favours this model because it would favour competition between societies and price levels.
- *Online music providers.* Like the radio broadcasters, they favour option 2 because they would like to have an EU wide license for the aggregate EU repertoire. In addition to this, they favour the introduction of a mandatory dispute resolution mechanism.
- *The European Consumers' Organisation* (BEUC). BEUC aims to establish consumer choice at attractive prices. A good price for online music services, means a good price for consumers. BEUC mentions that option 2 of the Study might have been a viable basis to address the current problems of collective management. With regard to option 3, BEUC points out the risk that commercially active CRMs might not be able or willing to support national artists on the margins of commercial viability when this option is followed. When minor, national artists are not considered, cultural diversity might diminish.

Option 3 – give rightholders the additional choice of authorising a collective rights manager for the online use of their musical works across the entire EU – is favoured by:

- *Music publisher's community*. Some music publishers already announced that, whatever the outcome of the stakeholder consultation, they will withdraw their repertoire from the existing reciprocal

agreements and tender the repertoire for a single EU wide license.

- *Independent record labels*. These record labels favour option 3 because this would enable them to establish their own CRM.

Two groups need to be mentioned separately here: first, the performers' societies, because they are uncommitted to any of the proposals; and secondly, the mobile network operators, because they favour a combination of option 2 and option 3 with a dispute resolution mechanism. The mobile network operators state that commercial users should have the possibility to choose between obtaining license rights directly for the entire EU, and via reciprocity agreements for the remainder of the repertoire.

Commission proposal and justification (Chapter 7)

The different views expressed regarding the Study resulted in a proposal by the EC in which the parallel deployment of the business models in option 2 and option 3 is embedded. In addition, the EC introduces a series of fundamental freedoms that should form the basis of the relationship between rightholders, CRMs and commercial users.

According to the EC, commercial users should be able to obtain multi-territorial licenses for the entire EU irrespective of the Member State of residence or nationality of either the CRM or the rightholder; the categories of rights and the territorial scope should be defined in the license; and CRMs should enhance transparency, for instance by publishing repertoire and applicable prices.

Rightholders should be able to determine the categories of rights and the territorial scope entrusted for collective management; they should be able to withdraw rights from existing agreements with CRMs in order to join the CRM of their own choice, irrespective of the Member State of residence or nationality of either the CRM or the rightholder.

In addition to the principles mentioned above, the EC also introduces rules on governance, transparency and accountability that CRMs should adhere to. These rules include the following principles:

- CRMs should grant commercial users licences on the basis of objective criteria and without any discrimination against users;
- CRMs should be obliged to distribute royalties to all rightholders or categories of rightholders they represent in an equitable manner;
- CRMs should establish clarity among themselves and vis-à-vis commercial users as to which rightholders they represent and update this information on a regular basis;
- CRMs should specify vis-à-vis all the rightholders they represent, the deductions for purposes other than for the management services provided;
- Management contracts between CRMs and rightholders for the EU-wide management of musical works for online use should also specify whether and if so, to what extent, there will be deductions for purposes other than for the management services provided;
- The relationship between CRMs and rightholders, whether based on contract or statutory membership rules should comprise the principle that a CRM treats domestic and non-domestic rightholders or categories of rightholders equally in relation to all elements of the management services provided;
- The relationship between CRMs and rightholders, whether based on contract or statutory membership rules should contain the principle that rightholders' representation in the internal decision making process is fair and balanced namely commensurate with the economic value of their rights;
- CRMs should report regularly to all rightholders they represent whether directly or under reciprocal representation agreements on licences granted, tariffs applicable and royalties collected and distributed;
- Member States are invited to provide for effective dispute resolution mechanisms in relation to tariffs, licensing conditions, entrustment of online rights for manage-

ment and withdrawal of online rights available to commercial users and rightholders in their territories.

Recommendation

The Impact Assessment formed the basis for releasing the Recommendation (European Commission 2005d and European Commission 2005f). It is important to note what the status of such a document is. The Recommendation, which is based on Article 211 EC Treaty and is directed at Member States and all economic operators that are involved in the management of copyright and related rights in the EU, can be interpreted as a signal to stakeholders that they will need to do something to improve the current situation in a way that will enable online music services to license music in an easier way. A Recommendation is not binding for the concerned parties. However, it does have a certain persuasive character since it forms the last possibility for the parties concerned to introduce self- regulation before the EC issues binding legislation.

The different views from stakeholders on the issue have resulted in a Recommendation which does not impose the implementation of either option 2 or 3 upon the concerned parties. Rightholders and commercial users of copyright-protected material should be given a choice as to their preferred model of licensing. To achieve a better functioning of the existing reciprocal agreements and to make option 3 a possibility, the EC proposes the elimination of territorial restrictions. In addition, customer allocation provisions in existing reciprocal representation agreements should be eliminated. Furthermore, rightholders who do not wish to make use of reciprocal agreements to manage their repertoire should be offered the additional option to tender their repertoire for EU-wide direct licensing. Lastly, the Recommendation contains a number of principles to which CRMs should adhere in order to introduce a culture of transparency and good governance enabling all relevant stakeholders to make an informed decision on the licensing model best suited to their needs. These principles correspond to the principles mentioned in Chapter 7 of the Impact Assessment and are applicable to all CRMs, irrespective of whether they manage rights according to option 2 or option 3.

A bit of discussion

Some issues resulting from the Impact Assessment and Recommendation are worth mentioning here.

Attractiveness of DRM

The statement of the EC according to which rightholders will take into account the DRM solutions applied or imposed by the CRMs to protect and monitor their rights in the most efficient way, suggests that all rightholders favour the use of DRM. One indication in support of this statement is the fact that legitimate downloading services are becoming more and more popular. However, more and more artists are publicly rejecting the use of DRM (and, more specifically, copy protected CDs which hinder the transfer of the bought CD to an MP 3 player) by their record companies. Use of DRM might thus also drive a certain artist away from the record company. In the future, more discussion between rightholders and the party applying a DRM concerning the possibilities of applying a certain DRM is needed.

Choice as an advantage

The EC wants to give rightholders a choice when joining a CRM. Do rightholders actually want to have a choice, do they have the knowledge to make a profound choice and, moreover, would they use the opportunity to join a CRM not based in their territory? Big rightholders, like record companies, are more likely to have the knowledge to make a profound decision to choose (or even establish) a CRM than individual rightholders. In addition to this, the right of the rightholder to withdraw licensed rights from a CRM at any given time does not enhance certainty amongst online music services. Only a register which is updated regularly (probably at least daily) might give a good overview of who is represented by which CRM for which rights. If there is no such on-going registration, an online music service might address a certain CRM who does not represent a certain rightholder anymore.

Reduction of costs

It remains also to be seen whether implementation of option 3 indeed does diminish the costs for online music services when offering digital music. The online music service still would have to conclude several licenses if a rightholder grants different CRMs the right to license certain rights in a designated area and when no reciprocal agreements are in place.

Bottom line

Whether one supports option 2 or option 3, it is now up to the stakeholders to implement either of those options and to improve the current situation. Whatever stakeholders decide to do, the implementation of the principles to which CRMs should adhere, will definitely improve the greater good of transparency!

Sources

- European Commission (2005a): Commission staff working document (2005): Study on a community initiative on the cross-border collective management of copyright; http://europa.eu.int/comm/internal_market/copyright/management/management_en.htm
- European Commission (2005b): Press Release IP/05/872 of 7 July 2005: Music copyright: Commission proposes reform on Internet licensing; http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/872&format=HTML&aged=0&language=EN&guiLanguage=en
- European Commission (2005c): Impact Assessment, Commission staff working document, Annex to the recommendation from the commission on performing cross-border management of copyright and related rights for legitimate online music stores; http://europa.eu.int/comm/internal_market/copyright/management/management_en.htm
- European Commission (2005d) Commission Recommendation on collective cross-border management of copyright and related rights for legitimate online music stores; http://europa.eu.int/comm/internal_market/copyright/management/management_en.htm
- European Commission (2005e): Communication from the Commission on Impact Assessment, COM (2002) 276, 5.6.2002
- European Commission (2005f): Press release IP/05/1261 of 12 October 2005: Music copyright: Commission recommendation on management of online rights in musical works; http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/1261&format=HTML&aged=0&language=EN&guiLanguage=en
- Groenenboom (2005): Improving cross border licensing practices for online music stores, INDICARE Monitor, Vol. 2, No 7, September 2005, http://www.indicare.org/tiki-read_article.php?articleId=139

About the author: About the author: *Margreet Groenenboom* is project researcher at the Institute for Information Law, University of Amsterdam. She specialises in copyright law, patent law, trademark law and law & information technology. Contact: groenenboom@ivir.nl

Status: first posted 24/11/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=156

DRM researchers do not disregard consumer acceptability any more

A report on the fifth ACM workshop on Digital Rights Management

By: Kristóf Kerényi, SEARCH laboratory, Budapest, Hungary

Abstract: INDICARE was present at the 2005 ACM DRM Workshop in Alexandria, VA, to monitor what has changed during the past year in the field of DRM technology. Although the attendance of the workshop was not too high, we heard quality presentations, and a little bit surprisingly the focus has moved from completely technical to multidisciplinary, and much heed was given to consumer acceptability of DRM solutions.

Keywords: conference report – consumer research, DRMS, fair use, rights expression language, standards, technical protection measures

Introduction

Having been at the last year's DRM workshop organized by ACM (Association for Computing Machinery) (cf. Kerényi 2004), I looked forward to visiting the 2005 event organized in Alexandria, Virginia. This time the workshop, being part of a week-long event, the 12th ACM Conference on Computer and Communications Security, was organized in a more prestigious place than last year, the Hilton Alexandria Mark Center. Therefore I was surprised, that compared to the previous workshop, the number of the audience was approximately halved. The around twenty participants came from all over the world, mostly universities, but there were some representatives from the tech industry (Microsoft, Motorola).

As the name of the enclosing event suggests, I expected the presentations to havie mainly technical focus, but the title of the first two presentations (cf. event web site, workshop program) suggested a stronger consumer-related view. As the whole event was introduced, the workshop this year promised a "comprehensive intellectual view", mentioning the legal and market-related questions of DRM beside the expected technical focus.

Opening block – Legal issues and fair use

Alapan Arnab from the University of Cape Town talked about the well known controversy, that DRM, which was meant to be an active protection of copyright, as opposed to the historic passive enforcement, does not actually implement the fundamentals of copyright law. One of the most salient signs is that current systems do not allow fair use. As he said fair use was "a feature for lawyers", that computers, more specifically Rights Expression Languages, could not express. Therefore he concluded that "fair use was unsuitable for DRM". Instead he proposed that "fairer use" could be achieved, than what is available at present.

Arnab discussed the question whether DRM systems are rather similar to buying or licensing. He stated that DRM systems will never be able to enforce core protection (copying, redistributing), they can only restrict usage. Thus, if we drop the old view of 'buying music just as one used to buy a CD' and look at today's 'buying content from the on-line store' as licensing (basically a contractual process), then consumers will not necessarily be in a worse position. However, for contracts it is necessary, that both parties can provide their input, and agree on the terms and conditions under which the deal will be made. Current DRM systems, he said, do not allow the users any input on the terms of the usage licenses. For this, he proposed two different solutions, which could contribute to achieving fairer use.

First, he talked about negotiation of licenses. He described a protocol, based on which the end user and the license server could conduct the negotiation process, and by which e.g. different prices could be paid for different sets of rights. He proposed that instead of a separate language for negotiation, RELs should be extended to be able to support bi-

directional requests. (see also Rump, 2004) He also proposed extensions to the two most widespread RELs, ODRL and XrML, to make such negotiation of terms possible.

The second solution Arnab proposed was credentials-based. He said that credentials-based systems were not new, and such functions could be achieved in DRM systems, too. A simple example of credentials-based access could be that for average users some form of license is granted to a piece of writing, in which any derivative work is forbidden, but those who have a journalist credential are allowed to excerpt. Naturally trusted credentials servers are required for strong identity management in order to maintain security of the system. Arnab again examined both ODRL and XrML, and concluded that the latter was ready for credentials-based use, and proposed an extension for the first one to be compatible with this approach.

Rei Safavi-Naini from the University of Wollongong, Australia, presented research done by four fellows, one dealing with computer law and three sociologists. She analyzed fair use and *fair dealing*, as similar concepts in many countries, including Australia and also appearing in some EU documents. She gave a detailed background about the history and law cases in connection with fair use and personal use.

Safavi-Naini talked also about the social context of music and new media. The authors examined several surveys, and concluded that music was very important in society, because "music and talk about music is a way of constituting and maintaining friendship networks". They also conducted in-depth interviews with 23 consumers, somewhat similar to what INDICARE did (cf. references). The authors found out that both listening alone *and* sharing one's vision with friends was a basic social need. Thus she concluded that DRM systems need to encourage sharing and exploring new music, because this is what people always wanted. Safavi-Naini said that exploration of new music based on sharing often leads to purchase. Thus, revenues can be collected by different means, e.g. with the purchase of concert tickets, T-shirts, CDs, etc.

The key recommendation of the presentation was that "DRM systems should concentrate on how sharing and exploring new music can lead to a purchase, rather than try to stop a core music activity". DRM system designers should address user requirements in the area of file sharing, and make it possible for users to legally exchange music.

Interoperability

At the workshop we had also quite some presentations regarding interoperability, one of the questions that interest consumers most. The three speakers who touched the topic the closest each had a different view of how to achieve this goal.

Pramod A Jamkhedar, from the University of New Mexico, continued research that he had presented in the previous year's conference. At that time he had talked about creating a layered architecture for DRM and standardizing the function of the layers (cf. Kerenyi 2004). This year he analyzed what is necessary for achieving interoperability (interfaces, protocols, standards that should be developed). Jamkhedar's view was that standardization does not have to happen all at once; while today's DRM systems are monolithic, and in the future the aim is to create highly interoperable system, there will be a gradual change through intermediate levels of interoperability.

Sam Michiels, a researcher from the Katholieke Universiteit Leuven took a very different approach: instead of defining layers and dividing DRM functionality in a vertical manner, he looked at the functionality that DRM systems provide. Michiels analyzed state-of-the-art DRM technologies and extracted from them high level usage scenarios with respect to consumers of content, producers and publishers. He identified seven subsystems which are, or should be common to all different systems. These are Content Service, License Service, Access Service, Tracking Service, Payment Service, Import Service and Identification Service.

Micheils concluded that today's DRM systems lack a generic software architecture that supports interoperability and reuse of specific DRM technologies. He proposed that

the identified functions and key services should be located in an overall software architecture for DRM, and the different functions and sub-services of DRM should be standardized. This could also contribute to the gradual change to full interoperability, and provide a way for newcomers to the market to step in with just one of the functions newly implemented and using existing subsystems for the other key services. By not having to re-implement the whole DRM architecture every time one has a new idea for one of the six functions, the market could open up to new ideas and grow faster, to the benefit of consumers.

While the previous two speakers presented "just research", and had no intention to promote actual standardization, *David W. Kravitz* from Motorola talked about a real device which could help achieve interoperability. He introduced the Rights Issuer Module (RIM), a central device in one's home entertainment system, which achieves functional interoperability by acting as a content and rights object translator between the "upstream device" (could also be the content provider) and the "downstream device" (this is the device receiving the content and rights). Motorola's aim when designing the RIM was to create a supplementary system with the help of which one can easily move content among devices with minimal or potentially even no change to existing players, and that was secure, while at the same time reducing robustness requirements for home devices.

Technical research going on

Just to touch on other topics mentioned at the workshop, we also had presentations about broadcast encryption, watermarking, and software protection techniques. *Markus Rohe* from the Ruhr-Universität Bochum introduced a secure digital rights distribution infrastructure, where customers can verify the legality of a license. This is important, when digital content is used for important calculations, and accuracy of data is crucial, and this infrastructure can guarantee liability of the content provider. *Andreas Matheus* from the University of the Federal Armed Forces Munich talked about extending DRM systems to the geospatial domain – with GeoXACML Matheus successfully added location information to both content and rights, which can be important if heterogeneous and distributed geodata are to be used at the same time, or usability of licenses can vary based on the location of the consumer.

Microsoft's DRM vision

The liveliest discussion emerged, when *Andrew Moss*, a Windows strategist from Microsoft stepped on stage and gave a less technical and more visionary speech. After his talk, attendees of the workshop asked questions about Microsoft's vision and to me it emerged that consumer acceptability is indeed a very important question for the "bigs". Moss emphasized the importance of simplicity of DRM systems. He said that most consumers are not engineers therefore simplicity of solutions is one of the most important points when designing a DRM system. Therefore the best DRM is invisible, "if you realize it is there, they do something wrong". Moss said that "the challenge now is not too much in technology", instead he identified today's key disputes as privacy, accessibility, ease of use, interoperability and device-to-device availability.

Bottom line

Compared to the results of last year's similar DRM workshop by ACM where researchers did not pay much attention to consumer acceptability, it seems that now the approach of both researchers and technology providers have changed, and today the end user, and his wishes are in the focus of research.

Sources

- Dufft, Nicole et al. (2005): Digital Music Usage and DRM. Results from an European Consumer Survey. INDICARE; http://www.indicare.org/tiki-download_file.php?fileId=110
- Kerényi, Kristóf; (2004): Content protection comes first. A report about the Fourth ACM Workshop on Digital Rights Management. INDICARE Monitor, Vol. 1, No 6/7, December 2004; http://www.indicare.org/tiki-read_article.php?articleId=57

- Rump, Niels; Barlas, Chris (2004): From couch potato to active consumer. Potential impact of bi-directional Rights Expression Languages. INDICARE Monitor, Vol. 1, No 4, September 2004; http://www.indicare.org/tiki-read_article.php?articleId=42
- The website of the workshop is available at http://www.titr.uow.edu.au/DRM2005/

About the author: *Kristóf Kerényi* is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His interests include mobile and wireless IT security, as well as technological aspects of DRM. He received a MSc in computer science from BUTE. Contact: kerenyi@mit.bme.hu

Status: first posted 25/11/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=157

Governing the interrelation of information markets and the public domain. A review

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The journal article reviewed here (Holtgrewe 2005) attempts to explore the changing boundaries and interrelations of information markets and the public domain in the light of digital technology, digital goods and changing intellectual property regimes. The music sector and scientific publishing are the cases studied in more depth. The concepts used are derived from a sociology of knowledge understood as an "interactionist" and "constructivist" endeavour.

Keywords: review – intellectual property, music markets, scientific publishing, sociology of knowledge, copyright law, open access, consumer behaviour

Introduction

By and by changing intellectual property regimes – copyright and DRM included – are appearing on the radar of social scientists. The input of social science to the many-voiced transdisciplinary dialogue about these issues – INDICARE being one place among others for this exchange – is welcome. Social scientists as observers promise to generate a broader perspective beyond the narrower view of stakeholders. The article by *Ursula Holtgrewe* which we review in the following is an interesting case in point.

Some basic assumptions

Holtgrewe starts from two premises: First, the commercial sector and the public domain do not follow the either-or-rule of a "zero-sum game". What has to be understood is the interrelation between both. The public domain is understood here in a broad sense as "the sphere of freely accessible knowledge and/or cultural goods that may be circulated, used and further developed by anyone" (p. 41). Second, intellectual property regimes are a means to govern the relation between commercial and public information provision: And as such they become "a dynamic object of action, discourse, power and influence themselves" (p. 40).

Her reasoning is meant first of all to challenge the "essentialists" who opt for either the market or the public domain. Second, she argues against current legislation, the European Copyright Directive and its national implementation in Germany in particular, which she perceives as a threat to the (once) beneficial balance between the commercial and public sectors.

What I find most interesting, however, is her claim in the field of social theory, namely to overcome what she calls "digital neo-Marxism" (p. 45). Digital neo-Marxism basically sees at work the "capitalist contradiction between forces and relations of production" (p. 44). It exists in two variants, the optimistic one highlighting the inherently free and cooperative logics of new technology, while the pessimistic one sees the inten-

sification of capitalist exploitation logics. "At this point, the perspective of the sociology of knowledge brings in a contrasting view. It emphasises the contextual, processual, potential and generative character of knowledge. Here the focus is on the practical and embedded utilisation of knowledge" (p. 45).

In order to demonstrate some benefits of this sociological perspective, she takes a closer look at two concrete social "contexts": the music sector and scientific publishing. The differences she identifies between the two sectors are indeed very interesting.

Comparing the music sector and scientific publishing

While the music sector might appear at first glance as governed by markets, and scientific publishing as governed ultimately by the "communist" (Merton) rules of scientific knowledge production and dissemination, in reality both fields present patchworks of mixed economies. In the music sector for instance the creation of music and performing are often "not purely for-profit" (p. 46), and important parts of distribution and consumption take place as non-commercial "social exchange". In addition levy schemes and collecting societies have their role.

In scientific publishing knowledge production is mostly public, the physical production and distribution however mostly commercial, although authors often do the pre-press work. Archiving is a public activity when done by libraries and a commercial one when done by databases providers etc.

Following Holtgrewe, in both fields the institutional arrangement is in crisis. In the music sector consumers have been empowered by new technical possibilities (provided by the ICT industry) and they have leveraged this potential by enhanced forms of "social exchange" – think of file sharing networks for instance. High prices for CDs to be paid by the end-users themselves are regarded as an important incentive to go for free content. At the same time, as she observes, the music industry was reluctant to make use of the technical potential and to come up with new attractive business models. Instead the industry followed a conservative strategy relying on restrictive legal regulations and technical protection measures. All in all the music industry has manoeuvred itself into a crisis of demand.

In contrast in scientific publishing the "serials crisis" (or "journal crisis"), a supply crisis, is the starting point. This crisis made obvious that the basic institutional arrangement with commercial publishers on the one hand and libraries on the other hand – as bridge between the commercial publishers and the public domain – did not work well any more. The new technical possibilities are used now to redefine the boundary between for-profit and non-profit activities in this sector. Pre-print archives, open access journals etc. are indicators of the attempt to get larger parts of publishing back into the public domain. The attitude of end-users and industry in this field is rather distinct from the music sector: Scientists as users did not protest significantly against the established arrangement for a long time, because they often do not have to pay themselves for the information needed. The university or research institution pays. From the point of innovativeness, commercial publishers were early birds starting many electronic services, especially databases, even before the invention of the Internet, and were thus prepared when the new network technology appeared.

Discussion

Overall the article shows that context matters and that a comparison of different fields is a worthwhile exercise. But there are more topics Holtgrewe's "exploratory study" (p. 40) touches upon. I would like to point out four worth further debate.

- Holtgrewe warns not to overestimate the Open Access movement. It took a long time for authors to become aware of the serials crisis and the changes happening, and as long as reputation is linked with commercial journals the general picture will not change too soon. This however may differ from discipline to discipline. With respect to the OA movement she misses "institutional imagination" when developing open access platforms, e.g. to "experiment with more open forms of

evaluation instead of peer-review" (cf. p. 53).

- With reference to *Michel Callon* she points to the fact that technical accessibility is not yet "open access" as it does not *per se* avoid exclusion from knowledge. "The very contextuality of knowledge makes it exclusive" (p. 45). Additional information work is required to make scientific knowledge digestible and usable for other groups.
- Drawing attention to "social exchanges" – to address non-commercial exchanges between colleagues, family, friends etc. – is an important step. It adds a level of consumption and information use transverse to both commercial exchanges and exchanges in the public domain. I doubt however that a broad generic term like "social exchange" is very helpful to address this level.
- A further interesting aspect she touches is the contradictory policy of governments, who on the one hand support OA initiatives and on the other hand comply with the demand of commercial lobbies when it comes to legal regulations.

Bottom line

The article reviewed is strong in exploring the intellectual property regimes in fields as different as the music sector and scientific publishing, and in providing a picture of the patchwork of for-profit and non-profit activities in these fields. However, the article does not live up to its ambitious claim of a sociology of knowledge which makes the utilization of knowledge the centre of observation.

Sources

- Holtgrewe, Ursula (2005): Intellectual Property, Communism and Contextuality. A non-essentialist exploration of German digital copyright and the public domain. Science, Technology & Innovation Studies, Vol. 1, July 2005, pp. 39-57; http://www.sti-studies.de/articles/2005-01/holtgrewe/Holtgrewe-STI-2005.pdf

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was Visiting Scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he acts as editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 24/11/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=154

Editorial of INDICARE Monitor Vol. 2, No 10, 23 Dec. 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: In the editorial we announce the report of the 3rd INDICARE Workshop about "Fair DRM Use", hint to the call for contributions to the 5th INDICARE Workshop about "Human Factors of DRM" (Budapest 19/01/06), and express our wish for more INDICARE Monitor articles from Northern, Southern, and Eastern Europe. The five articles published in the December issue cover BEUC's reasons for its Campaign on Consumers' Digital Rights, a review of a study commissioned by BEUC testing the interoperability between online music stores and portable players, an introduction to DVB-CPCM, the content protection and copy management system proposed by DVB for digital broadcasting, and finally a conference report about DRMTICS 2005 and a second about Axmedis 2005.

Keywords: editorial – INDICARE

INDICARE news

The *3rd INDICARE Workshop* about "Fair DRM Use" was organized by the Institute for Information Law (IViR) and took place in Amsterdam, 28 May 2005. Meanwhile *Mara Rossini* and *Natali Helberger*, both from IViR, have produced a concise and well written workshop report (Rossini and Helberger 2005), which is available online. It summarizes and synthesises presentations and debates. While the first part of this 18-pager deals with consumer expectations and consumers' legitimate interests, the second part is about political and regulatory options for consumer protection.

The *5th INDICARE Workshop* about "Human Factors of DRM", scheduled for the 19th of January 2006 in Budapest is organized by INDICARE partner SEARCH. The aim of the workshop is to put the consumer and his needs in focus analysing DRM-protected offerings and devices from a human factors point of view. Special attention will be given to the access problems of potential users living in less developed countries and groups with special needs like disabled persons. Don't hesitate to contact the organisers if you would like to present at the workshop or to participate. To learn more about the workshop, please have a look at the "Call for presentation" at our website (cf. sources).

Towards the end of the year, when wishes are more likely to come true, I would like to express our INDICARE Monitor wish for the next year: users and consumers of DRM systems from Northern, Eastern and Southern Europe contribute to the INDICARE Monitor! It is meant to be a truly European online journal covering experiences and opinions from all over Europe. Help us to better achieve this goal!

About this issue

BEUC's criticism of European policy

BEUC, the European Consumers' Organisation, and other consumer organizations have been denouncing for a long time shrinking consumer rights in the digital environment - the Sony BMG scandal being just the tip of an iceberg. What bothers BEUC most as a European high-level interest group is apparently the feeling that their arguments remain - so far - unheard by European policy makers. Consequently they started a Campaign on Consumers' Digital Rights. The article by *Cornelia Kutterer* is however much more than a description of this campaign. It is but a serious attempt to investigate cases of ongoing policy making showing how the interests of consumers are ignored or weakened in these processes. An essential weakness of European policy is seen in the conflation of commercial infringement of copyright (piracy) and non-commercial copyright infringement, ending up with a notion of piracy as first of all non commercial infringement.

Intertek's interoperability study

Kristof Kerenyi, SEARCH, contributes a knowledgeable review of an interoperability

study performed by *Intertek Research and Performance Testing* and commissioned by BEUC. UK-based music services and widely available digital music players were compared and tested with a focus on interoperability of file formats and DRM formats. The main results are presented in the review. The review highlights the value of the study as easy to read "educational material" for the public making aware of DRM systems' limitations today - including hints how to achieve interoperability nonetheless.

DVB's Content Protection & Copy Management specifications

Chris Hibbert, Vice President Media Technologies & Standards with Walt Disney Television International, gives an excellent introduction to the Content Protection & Copy Management (DVB-CPCM) system developed by the Digital Video Broadcasting Project and published in November 2005. More precisely the first three elements of this specification have been published. DVB, established in 1993, is today a consortium of c. 300 companies from more than 35 countries committed to develop pan-European open standards for digital broadcasting.

The article does not go into technical details, but gives a high-level overview of the main features of the DVB-CPCM specifications and the work still ahead. Apart from the clear presentation of a rather complicated subject, I do appreciate that Hibbert also explains the context of this standardisation effort: the changing scope of DVB activities, the motivations behind DVB-CPCM, and even lines of conflict.

Conference reports

Rei Safavi-Naini, *Wanqing Li* and *Nicholas Sheppard* all involved in the organisation of DRMTICS 2005 provide you with a comprehensive conference report. DRMTICS, Digital Rights Management: Technology, Issues, Challenges and Systems, took place in Sydney from October 31 to November 2. The interdisciplinary character of the conference is worth highlighting. As the full proceedings of the conference will be available in Springer's Lecture Notes in Computer Science later in 2006 this report is a good opportunity to get first hand impressions and an overview of the event.

Gergely Tóth, SEARCH, reports about Axmedis 2005, the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution taking place in Florence, November 30 to December 2. Although Axmedis is mainly a large European R&D project (FP6 Integrated Project) addressing cross-media production and distribution, the conference was interdisciplinary in nature. This was achieved by organising additional panels and sessions devoted to user and consumer aspects of digital media and DRM. For instance a panel was organized on collecting societies, the EUAIN, the European Accessible Information Network, organized a panel, and in particular the "digital goods workshop" (the third in a series), which addressed user and consumer aspects in digital goods markets, was incorporated in the conference framework. As the conferences proceeded in parallel sessions, the present conference report can of course not cover all. The good quality of the conference makes me therefore recommend the two printed volumes of the proceedings, which are already available.

As you will have noticed, this INDICARE Monitor is not published last Friday of a month as usual, but the last but one due to Christmas time. We wish you the very best for the holidays to come and the next year

the INDICARE team

Sources

- Rossini, Mara and Helberger, Natali (2005): Fair DRM Use. Report on the 3rd INDICARE Workshop Held on 28 May 2005 in Amsterdam; available at http://www.indicare.org/tiki-download_file.php?fileId=146
- 5th INDICARE Workshop on the Human Factors of DRM: CALL FOR PRESENTATION: http://www.indicare.org/tiki-page.php?pageName=WorkshopFiveCall

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in

Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 23/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=164

Some of the reasons for BEUC's Campaign on Consumers' Digital Rights

By: Cornelia Kutterer, BEUC, and Brussels, Belgium

Abstract: This article explains the reasoning behind BEUC's "Campaign on Consumers Digital Rights". Current international IPR policy, in particular that of the European Union is perceived as a danger to established rights of consumers. This opinion is put forward supported by a series of arguments and examples.

Keywords: opinion – consumer protection, data protection, digital television, DRMS, piracy, private copy – EU

Introduction

The ease of digital copies has challenged traditional business models by lowering the cost and effort of reproduction and distribution. Different business models for content delivery compete in a fast developing technological environment. As a result, values such as the protection of Intellectual Property Rights (IPRs) on the one hand and the protection of the private sphere and consumers on the other seem to be more and more at odds.

Even voices from industry confirm the threat. In the words of *Gary Shapiro*, president and chief executive of the Consumer Electronics Association (CEA): "In the rush to crack down on pirates, we risk eliminating a critical consumer right – the right to use copyrighted material, without the permission of the copyright owner" (quoted in Taylor and van Duyn 2005).

But generally industry tends to ignore the interests of consumers. A notorious example is Sony BMG's director for digital business, *Thomas Hesse*, who stated – when debate about the Sony BMG debacle over its intrusive DRM system heated up: "Most people, I think, don't even know what a rootkit is, so why should they care about it?" (quoted in Orlowski 2005; cf. Bohn 2005 for more debate on the Sony BMG debacle; cf. also Doctorow 2005a). It may possibly be true that many consumers are not aware of DRM (cf. the results of the INDICARE survey, Dufft et al. 2005), let alone the effects it may have on their private lives. But does that mean that they shouldn't care about it? Can we watch the societal shift from young people taping at home in a private sphere to a generation surveyed and criminalized?

Facing these threats, it seems astonishing to the naïve reader that *Charlie McCreevy*, Commissioner for Internal Market and Services, stated in a recent speech before the BSA (European-American Business Council/Business Software Alliance) that "the pure technology issues such as the robustness of the technology, the acceptance by consumers can be left to the market" (McCreevy 2005). Another example of the weak standing of consumer interests in public policy is the "EU-US Initiative to Enhance Transatlantic Economic Integration and Growth". While the Commission has acknowledged in a draft implementation paper of this EU-US Initiative that there is – in respect to DRM and technical protection measures - a need of "taking due account of public policy interests, such as the promotion of fair competition and consumer rights, with a view to identify best practices", in the final version

this sentence was deleted – due to US pressure (cf. EU-US 2005).

Consumer organizations have been denouncing for a long time shrinking consumer rights in the digital environment (cf. e.g. BEUC 2004) but remained so far unheard by European policy makers. It is against this background that on 10 November BEUC, the European Consumers' Organisation, launched a *Campaign on Consumers Digital Rights* supported by *Zusana Roithova,* Member of the European Parliament. The Sony BMG story merely underlined the necessity for this campaign and revealed that many of the issues addressed are not only "potential but unlikely risks" – instead – these risks have materialized. In the following we will point out some more European and international developments threatening consumers' rights by fostering technical protection measures and expanding criminal law. They all demonstrate the need for our campaign.

Blurring the boundaries between commercial and non-commercial copyright infringement

The entertainment industry has successfully watered down specific terms or extended their scope in commonly used language – such as piracy. What is piracy? It is an imprecise term for copyright infringement – in the first place – because it disregards the necessity to differentiate between non-commercial and commercial copyright infringement. While some "pirated content" is simply infringing (you upload a copy-protected music file on a P2P net without permission), other is commercially infringing (somebody sells an illegal copy). The impact of each is different. Conflating them under the "piracy" banner is nonsensical. By the way, conflating non-commercial infringement of copyright under theft is nonsensical as well.

In the 90s, the Commission was willing to distinguish commercial infringement of copyright (=piracy) from non-commercial copyright infringement:

> "Piracy … embraces the unauthorized reproduction of works protected by copyright or allied rights for commercial purposes as well as all subsequent commercial dealing in such reproductions. *The commercial purpose* and frequently the scale on which the activity is carried out are characteristic features which distinguish the practice from other forms of unauthorized reproduction or use such as home copying. Piracy in this sense includes bootlegging, that is, the unauthorized recording of performances and the subsequent marketing of copies of the recording. It is frequently associated with counterfeiting, that is, unauthorized use of a legitimate product commercial presentation, in particular, its trade mark or some other protected indication" (EC 1988).

Today, it appears that the Commission no longer distinguishes these two different types of infringement. But blurring these boundaries leads to excessive reactions that may have deep, irreversible and adverse effects on our society, technological development and the private sphere.

In a highly controversial and often hostile debate about the scope of IP protection, recent developments in the political debate tend to be excessive, disproportional, lopsided and do not take into account the existence of many discussions on how to improve creativity, access to knowledge and the legal use of technology. Instead, the law of unintended consequences is being provoked. Some examples:

Criminalization of consumers

In a recent proposal adopted by the Commission in July 2005, the Commission aims at introducing and aligning national criminal law provisions against infringements of IPRs. Under the proposal, infringements of any intellectual property rights are treated as criminal offences if undertaken intentionally and on a commercial scale. Similarly, attempting, aiding and inciting such infringements are considered criminal acts.

The problem is that the definition of "commercial scale" is not set out, and does not explicitly require financial benefits, profit or a commercial motive for activities to be identified as taking place on a "commercial

scale". This may straightforwardly lead to private non-commercial (but infringing) uses being criminalised as of potentially commercial scale (the issue – rejected during the 2004 Enforcement Directive debate – is thus back on the agenda). The inclusion in criminal behaviour of activities collected together under "aiding or abetting and inciting such infringements" is imprecise and far too inclusive of activities that are entirely legal. Thus, it is possible that an email noting the existence of a piece of peer-to-peer software might be regarded as an incitement to infringe intellectual property rights.

Data retention

At the time of writing, the European Parliament is discussing and adopting a controversial compromise proposal to revise Article 15 of EC Directive 2002/58 that will introduce extensive common rules on data retention (On 14 December, the European Parliament approved at first reading (by 387 votes to 204 and 30 abstentions) the proposal for a directive on telecommunications data retention in the fight against terrorism and organised crime) despite the fact that the European Data Protection Supervisor and the Article 29 Working Party of European Privacy Commissioners have repeatedly stated that the case for retention has not been made and that the scope of that proposal is not proportionate (ARTICLE 29 Data Protection Working Party 2005): The European Data Protection Supervisor has also stated in his opinion, the mere existence of data might lead to increased demands for access and use by industry, law enforcement authorities, and intelligence services.

In the first place, data retention was considered necessary to combat terrorism. The adopted compromise foresees access to this data to combat all serious crimes (a term to be specified by the Member States). The CMBA, Creative and Media Business Alliance, however, lobbied strongly to include all crimes:

> "The scope of the proposal should include all criminal offences. The Directive, as proposed, is limited to the prevention, investigation, detection and prosecution of serious criminal offences such as terrorism and organized crime (Article 1.1). The position of the CMBA is that the scope of the proposal should be extended to all criminal offences. Limiting the proposal to serious offences would hamper the effectiveness of the Directive and the enforcement activities for other forms of criminal offences. Once an illegal activity is considered as a crime in a Member State, the enforcement authorities should have adequate means to prosecute it" (CBMA position on data retention of 22 November 2005).

CMBA would like to use a piece of legislation intended to fight terrorism in order to get hold of P2P-users that infringe copyright (cf. Cronin 2005). Obviously, non-commercial infringement of copyright must be made a crime in the first place.

Internet Services Providers' control of data

Other initiatives also aim at getting hold of the same data. A group of entertainment industry and Internet Service Providers is discussing with the European Commission – in a so-called "Sherpa group" – how best to cooperate to fight piracy (here it seems, the term piracy is used ***only*** for non commercials infringements).

The group is seeking to develop a charter on best practices in order to fight unauthorized file-sharing. The envisioned system would entail a graduated response system ultimately shutting down Internet connections of customers who engage in unauthorized file-sharing. The CMBA issued a statement on the charter on 2 November: "At its core, it should consist of a couple of escalating notices to infringers, culminating in termination, or at least suspension, of subscriptions for recidivists" (CMBA position paper on a EUropean Charter for on-line content of 2 November 2005). A similar procedure in France involved automatic systems to detect copyright infringement on peer to peer networks, and to force internet service providers to translate a given IP-address into an e-mail address and forward a 'pedagogical' e-mail message from the societies to their customer before commencing civil or criminal actions. But the French Data Protection authority

CNIL strongly rejected this approach as being disproportional (cf CNIL 2005).

Using ISP's and their contracts as enforcement vehicles raises a number of issues not least privacy but the CBMA statements on privacy wipes away these concerns: "It has become fashionable for some to claim data privacy constraints to plead against effective actions to tackle infringing activities by individuals. ….. Data protection should not be an impediment to the reasonable retention, preservation and access to evidence for legitimate purposes. It is essential to ensure that infringing activities are not protected by anonymity" (ibid.) The group further tackles liability provisions in the E-commerce directive: "Such a step could serve as one indicator to justify benefiting from the safe harbor provisions of the Electronic Commerce Directive that limit the liability of certain intermediaries under certain conditions" (ibid). This coincides with the Commission initiative to set up an expert group (comprising member states) to discuss the development of the e-commerce directive, in particular regarding ISP liability provisions (a Commission study on this topic is foreseen, see http://europa.eu.int/comm/internal_market/e-commerce/index_en.htm). But take down notices have proven to have little effect, easy to abuse and to come with chilling effects (cf. Urban and Quilter 2005).

Traceability – DRM requirement

NAVSHP

Other initiatives tackle the traceability of data. On September 13, 2005, the "Networked Audiovisual Systems and Home Platforms" group (mainly comprising interested companies) released a paper called "NAVSHP (FP6) DRM Requirements Report (NAVSHP 2005). This is a set of technical and commercial requirements for developing DRM. The purpose of the document was to promote common understanding within the NAVSHP, which in their research work has to tackle the DRM issue, to allow discussion and mutual help on this very complex issue. While the Commission has made explicit that it will not be bound in any way by the output of this activity and that there was no direct discussion on policy, possible legal requirements, etc. – it has also acknowledged the document's deficiencies in these areas.

The DRM specifications require for example: "There is a need to give the DRM system the ability to later prove consumer selections or actions that need to be monitored, in front of a 3rd party. This information can only be disclosed to appropriate authorized systems, in specific and clearly announced cases." Other requirements also treat users as infringers. It has never been questioned whether DRM should include traceability requirements at all. (for criticism cf. Doctorow 2005b).

DVB

Similar attempts to describe DRM specifications are made by an industry group called the Digital Video Broadcasting Project (DVB). This is an industry-led consortium (with no consumer participation) of over 260 broadcasters, manufacturers, network operators, software developers, regulatory bodies and others in over 35 countries committed to designing global standards for the global delivery of digital television and data services. Its sub groups, CM-CP and TM-CPT, are working to develop the Content Protection and Copy Management (DVB-CPCM) system for managing distribution, copying and redistribution of television content (cf. in this INDICARE Monitor the article by Hibbert 2005), akin to the US "Broadcast Flag" which has been successfully stopped in a recent US court of appeal decision. DVB-compliant solutions will effectively hinder or prevent consumers from recording free over-the-air broadcasting for legitimate time-shifting usages (for criticism see Doctorow 2005c). It will be now submitted to ETSI standardization.

Bottom line

These recent developments and initiatives show that the balance between the rights of the right holders and the rights of consumers is neither achieved nor maintained but instead ever more threatened. Consumers' organizations have to be very vigilant in the near future. The European Commission has announced a review of a set of directives related to copyright, in particular the reform of copyright levies applied to equipment and

media used for private copying and a review of copyright term, above all, term for sound recordings are included in the review. Consumers' organizations will also need to look at the contractual side and pay high attention to abusive terms in services. An initiative report on consumer protection in the digital environment by the European Parliament could certainly help to address this issue.

A good sign came recently from The German Federal Supreme Court. It stated that "the necessary balance between the constitutionally protected rights of the right holders to exercise their rights and the constitutionally protected interest in competition, i.e. to be able to evolve freely outside that protected scope, would not be guaranteed anymore if the right holder could claim protection to an extent to which he is not entitled…" (BGH 2005). The court adds that this objective distinction between the scope of IP protection and the freedom of competition must also be balanced in regard to the means of enforcement. We believe that the statement is fundamental and should be reflected in all initiatives at hand.

Sources

- ARTICLE 29 Data Protection Working Party (2005): Opinion 113/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005). Adopted on 21st October 2005; http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf
- BEUC 2004: Digital Rights Management (DRM) – BEUC Position paper, X/025/2004, Brussels, 15.9.2004; http://www.beuc.org/Content/Default.asp?PageID=103
- BEUC (European Consumers, Organisation/Bureau Européen des Unions de Consommateurs), Brussels, Belgium http://www.beuc.org – http://www.consumersdigitalrights.org
- BGH (2005): BGH Case GSZ 1/04, July 15 2005.
- Bohn, P. (2005): Intrusive DRM: The cases of Sony BMG, StarForce and Microsoft. INDICARE Monitor, Vol. 2, no 9, November 2005; http://www.indicare.org/tiki-read_article.php?articleId=155CMBA (2005): CMBA statement of 2 November 2005 on 'A EUROPEAN CHARTER FOR ON-LINE CONTENT' (CMBA – A European Charter for on-line Content 2 November 2005) Hibbert, Chris: DVB-CPCM. First steps towards an open standard for a content protection and copy management system from the DVB. INDICARE Monitor, Vol 2, no 10, December 2005; http://www.indicare.org/tiki-read_article.php?articleId=159
- CNIL: Press release of 24 October 2005; http://www.cnil.fr/index.php?id=1881
- Cronin, David (2005): Music moguls want EU terror law to hunt pirates. European Voice of 24 November 2005, http://www.european-voice.com/archive/issue.asp?id=470 (registration required)
- Doctorow, Cory (2005a): Vaudeville offers a music lesson for Sony BMG. Financial Times (FT.com), December 11 2005 (registration required for download)
- Doctorow, Cory (2005b): Critique of "NAVSHP (FP6) DRM Requirements Report. Electronic Frontier Foundation 2005; http://www.eff.org/IP/DRM/NAVSHP/NAVSHP_critique.pdf
- Doctorow, Cory (2005c): Europe's coming broadcast flag: DVB CPCM is a stealth attack on Europeans' digital rights. Electronic Frontier Foundation 2005; http://www.eff.org/IP/DVB/
- Dufft et al. (2005): Digital Music Usage and DRM – Results from an European Consumer Survey, Berlin, May 2005; free download at: http://www.indicare.org/survey
- EC (1988): Commission of the European Communities. COM (88) 172 final . Green Paper on Copyright and the challenge of technology – Copyright issues requiring immediate action. Communication from the Commission. Brussels, 7 June 1988; http://aei.pitt.edu/archive/00001209/01/copyright_and_tech_gp_COM_88_172.pdf
- EU-US (2005): Implementation of the Economic Initiative of the June 2005 EU-US Summit: Joint EU-US Work Programme. Brussels, Washington, November 2005; http://www.europa.eu.int/comm/external_relations/us/economic_relations/joint_eu-us_work_prog.pdf
- McCreevy, Charlie (2005): European Commissioner for Internal Market and Services: Address to the EABC/BSA (European-American Business Council/Business Software Alliance) Conference on Digital Rights' Management. High level Industry Seminar/Global Industry Roundtable on Levies & DRMs. Brussel, 12 October 2005; http://europa.eu.int/comm/commission_barroso/mccreevy/docs/speeches/2005-10-12/euam_en.pdf

- NAVSHP (2005): DRM Requirements Report. Target release version: V1_.0; http://www.ist-avista.org/cg1_files/NAVSHP-DRM-CG_ADT_20051027.pdf
- Orlowski, Andrew (2005): Sony digital boss – rootkit ignorance is bliss. http://www.theregister.co.uk/2005/11/09/sony_drm_who_cares/
- Shapiro, Gary (2005, the CEA president and chief executive, in testimony before a US congressional committee. See in Financial Times 'Music industry asks whether fair use is fair play' by Paul Taylor and Aline van Duyn, 28 November 2005. http://news.ft.com/cms/s/2594a9f8-603a-11da-a3a6-0000779e2340,dwp_uuid=fcd3ba1e-2025-11d8-81c6-0820abe49a01.html
- Urban, Jennifer M. and Quilter, Laura (2005): Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act; (full research paper version of this study will be published in the March, 2006 edition of the Santa Clara Computer and High Technology Law Journal); http://mylaw.usc.edu/documents/512Rep/

About the author: *Cornelia Kutterer* holds the position of senior legal advisor at BEUC, the European consumer organisation. She is responsible for the legal department focusing on consumer protection law, contract law, passenger rights, intellectual property and information technology laws. She is a qualified German lawyer and holds a master's degree in information technology and communication laws. Contact: CKU@beuc.org

Status: first posted 20/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=162

Music services are incompatible

A research of what we already know

By: Kristof Kerenyi, SEARCH laboratory, Budapest, Hungary

Abstract: An independent institute was "commissioned by BEUC to investigate the limitations that may be present on purchased music downloads from major online suppliers and in particular, how these limitations restrict the consumer's traditional ability to transfer their music between platforms and players." INDICARE analysed the resulting Technical Report, and came to the conclusion, that the right findings were provided in the right form for the public, thus good "educational material" was produced for consumers.

Keywords: review – consumer expectations, consumer protection, consumer research, interoperability, music markets – United Kingdom

Independent consumer research

The European Consumers' Organization (BEUC) commissioned an independent institute, Intertek Research and Performance Testing, to perform an analysis of some of the UK-based music services and widely available digital music players and find out how interoperable they are, in other words the limitations, and "how these limitations restrict the consumer's traditional ability to transfer their music between platforms and players". This has been an intriguing question for consumers, most of whom have heard about the issue, but in the end they have had to accept the present situation of non-interoperable music download services.

Intertek chose four portable music players:

- an Apple iPod Photo was selected for its compatibility with Apple iTunes Music Store (AAC format files),
- a Creative Zen Micro was selected for its compatibility with MSN Music and Windows Media Player 10 (WMA format files),
- a Rio Carbon was selected for its WMA support (second player with WMA format files chosen because of WMA popularity, and also in order to test a second music store, HMV, using Microsoft's format) and

- a Sony Network Walkman for its compatibility with CONNECT Music Store (ATRAC3 format)

Each player was tested with the corresponding service, and players were also cross-checked to find out what level of interoperability exists, all of this from the layman's point of view.

Technical report

The result of the analysis was a technical report, which is now available for the public on a new web site titled Consumers Digital Rights (cf. sources), created as an information source for a wide range of readers, from politicians through journalists to consumers of DRM-protected content. "On this website we invite you to discover everything you always wanted to know about your consumer rights in the digital environment" – they declare.

Accordingly, the technical report is concise and easy to read, also providing basic information to those not really familiar with digital audio, DRM and related services. The report starts by giving a background to compressed audio, which, as opposed to traditional digital audio like CDs, makes new usages possible: "individual tracks or whole albums can easily be downloaded from the Internet where they can be purchased at lower cost and where new music can be discovered. Also, entire music collections can be copied and stored on a home computer/laptop or portable hard disc based audio file player" (p. 4)

In the following, different compressed audio formats are explained:

- mp3, as the most widespread format does not support DRM, and therefore it is not generally supported by major record companies
- WMA, Microsoft's file format does support DRM. Most music web sites have music available to download in this format, and it is also very popular with the manufacturers of portable players. The reason for the latter is that most modern PCs will already have the Windows Media Player (the player for this format), as the report says, though I have to disagree with this: I think that the main reason is that this is the only widespread technology that is free for everyone to license.
- ATRAC, Sony's file format, also supports DRM. This is said to provide the best sound quality for a given bitrate, but Sony so far has not licensed it to anyone, therefore it is a very proprietary format.
- AAC, the choice of Apple, is employed in the iTunes Music Store. While AAC is an open standard free to implement and use for everyone, Apple coupled it with its proprietary FairPlay DRM system, which makes it inaccessible for any of the few players that manage the compression format itself. (At this point the Technical Report is a bit confusing, saying that "AAC files can only be purchased through the iTunes web site" and suggesting that AAC is a file type supporting DRM. AAC in fact is just the compression method, unlike Microsoft's and Sony's compression-protection formats.)

Actual tests

The report moves on to the actual testing done at the research institute. They created accounts at the mentioned music stores, and bought a couple of songs, trying to play, burn, transfer (copy to a different computer) and transcode (convert to a different format) them. Importing songs to a different media player framework from where they were purchased and loading to portable devices were also main points of investigation.

To cut the long story short, each music store was quite comparable in terms and offerings. Each needed a special media player framework (Apple iTunes, Microsoft Media Player 10, HMV's own software and Sony SonicStage) to handle the music. They could be used for discovering new music, buying, organizing and playing songs and for transferring them to portable devices and finally exporting (burning to CD). Each compression method used about the same compression ratio (around the same file size for the same track). Apple and Sony provided only "permanent purchase" models with unlimited plays for a one-time payment and export options, while the two Microsoft DRM-based

systems additionally allowed monthly subscriptions where an unlimited number of songs can be played, but only as long as the subscription is maintained and after this period the songs become unavailable (the exporting option is in this case disabled).

The report analyses individual terms: number of PCs where purchased songs are playable, number of portable devices they can be transferred to and also the number of CD burns. There were some differences, but to me it seemed that the offerings were all liberal enough to not disturb the ordinary user. Terms were mostly correctly displayed before purchase, but in two cases the testers reported unexpected anomalies: in the MSN Music store "tracks were time restricted to 31/12/2099", which is a bad thing, but personally I do not consider this restriction very limiting to myself, the other was in the HMV store where the DRM system allowed a lot more than was stated before purchase – a nice surprise.

Compatibility

The authors of the report gave this chapter the title "File Compatibility" (page 11), but personally I would have preferred "system compatibility". They tried to import music bought from one system to another system's music library (the collection of music handled by the media player framework). It turned out that the two Microsoft DRM-based systems were (apart from one glitch) compatible with each other, but taking these two as one (since the employed technology was the same) protected music could not be transferred to other systems. This means complete lack of interoperability. Unprotected WMA files can be imported to iTunes and SonicStage, and thus transferred to an iPod, and a Network Walkaman successfully, but AAC and ATRAC files can not be transferred between systems. This is due to DRM-incompatibility rather than file-incompatibility in the case of AAC (since it is an open standard), and due to the incompatibility of both in case of ATRAC (since Sony uses a closed proprietary format) (pages 12, 13 and 14).

What I missed here was the analysis of whether MP3, OGG Vorbis, or other unprotected formats could be imported or exported to and from the respective systems.

Findings

When it comes to the analysis of DRM *systems*, the report becomes rather speculative. What is checked carefully is in particular the contracting terms. Not surprisingly the report discovers that different music stores have different conditions in terms of number of CD burns, portable players, etc.; usage restrictions are not clearly labeled, information on the web sites is not transparent and inconsistent across different music stores and licensing terms are difficult to understand; and by using proprietary formats download web sites can control what one can do with the music and the devices they will play on (cf. Summary, p. 2).

What is more astounding is that "the terms and conditions on these music stores allow the service provider to unilaterally change the terms", and "this would not even break the contract" (cf. Summary, p. 2). On the other hand, technically, it is also possible to change "limitations to a consumers existing collection", which means that in the future there is a possibility for music stores to retrospectively further restrict our purchased music – however, this would be technically challenging and highly unlikely (p. 16).

Yet what made me really wonder was that at the end of the report, in the Appendix, a detailed description is given about how to achieve artificial interoperability between the incompatible systems. More precisely, I was surprised to see this information made publicly available by a high level interest group. Burning the songs to CDs, and then re-ripping them with the target systems' media player frameworks might be a slightly inconvenient, but certainly effective way of lifting the DRM from the protected music (p. 19). And while the report says that this method is "time consuming", my opinion is that it is possible to create tools (and will therefore be such tools) which automatically do this.

Bottom line

The report talks about a media consultant, who said "My only confidence is that sooner or later the consumers will prevail by voting

with credit card against the worst systems" – the same conclusion which INDICARE has drawn in its State-of-the-Art Reports. Therefore beside the experiments carried out underlying the findings, there is nothing really special in the report that DRM experts were not aware of.

So I consider the main value of the research is that it is easy to read for the public, and comes to the right conclusions, therefore educating consumers about today's DRM systems limitations – and also on how to exercise their wish for interoperability by circumventing content protection.

Sources

- BEUC, (2005): Test on interoperability between online music stores and portable players – Summary. BEUC http://www.consumersdigitalrights.org/mdoc/x045cku2005e_13993.pdf
- Consumer Digital Rights web site, (2005): http://www.consumersdigitalrights.org/
- Intertek, (2005): Technical Report – Online Music Download Services. BEUC http://www.consumersdigitalrights.org/mdoc/OnlineMusicDownloadServices_TechnicalReport_90041.pdf

About the author: *Kristóf Kerényi* is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His interests include mobile and wireless IT security, as well as technological aspects of DRM. He received a MSc in computer science from BUTE. Contact: kerenyi@mit.bme.hu

Status: first posted 21/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=163

DVB-CPCM

First steps towards an open standard for a content protection and copy management system from the DVB

By: Chris Hibbert; Chairman, DVB-Copy Protection Technologies Group, London, UK

Abstract: After five years of work the Digital Video Broadcasting Project has published the first elements of its specification for a Content Protection & Copy Management (DVB-CPCM). This article introduces the background of DVB, explains rationale, scope and concepts of CPMC, and finally outlines next steps.

Keywords: review – authorized domain, broadband, conditional access, content protection, digital television, interoperability, stakeholders, standards, usage rights

Introduction

In November 2005 the Digital Video Broadcasting Project published a Blue Book, A094, containing the first three elements of its specification for a Content Protection & Copy Management (DVB-CPCM) system for use in consumer digital products and home networks.

The first three elements of the DVB-CPCM specification are: the CPCM Reference Model, which provides a technical and architectural framework for the CPCM System; the CPCM Usage State Information, which is content metadata that signals the authorised usage for a particular Content Item; and CPCM Abbreviations, Definitions and Terms.

Although the full system specification for CPCM is not complete the Blue Book is published for informational purposes and liaison with other interested standards forums. When completed the DVB-CPCM specification will be submitted to ETSI for standardisation.

This article will not go into a detailed description of the full functionality offered by DVB CPCM as the reader can obtain the

Blue Book by download from the DVB web site (DVB 2005). Rather the following is intended to give background to the DVB, why it embarked upon the work, and the major concepts embodied within the specification.

About the DVB

Today, the Digital Video Broadcasting Project (DVB) is an industry-led consortium of approximately 300 broadcasters, manufacturers, network operators, software developers, regulatory bodies and others committed to designing open standards for the delivery of digital television and data services. Although based in Europe DVB has members in over 35 countries.

The genesis of DVB was the debacle following the market failure in the early 1990's of the D-Mac satellite system which was mandated by the EC administration but not supported industry wide in Europe.

Persisting in the belief that pan-European standards for digital broadcasting will bring major benefits to consumers and manufacturers, the European Community administration turned to the industry and encouraged the setting up of a cross industry group to produce open specifications for standardisation based on industry consensus. This led to the formation of the DVB Project in 1993.

Initially the DVB concentrated on producing specifications for digital transmission systems for satellite, cable and terrestrial delivery and an interoperable Conditional Access system. These specifications have been adopted on a world wide basis resulting in the DVB becoming accepted as one of the leading specifications bodies. In recent times DVB has moved into the area of middleware and software producing the Multimedia Home Platform specification for interactive content and the Portable Content Format to provide common authoring to non-interoperable interactive platforms. Recently completed specifications also include DVB-H for broadcast delivery to hand held devices, DVB S-2 an updated and more efficient system for satellite delivery than its first specification which is now ten years old.

Work is ongoing within DVB on advanced encoding technologies and IPTV.

Since its inception the DVB Project has proven the value and viability of pre-competitive cooperation in the development of open digital television standards. DVB open standards guarantee fair, reasonable and non-discriminatory terms and conditions with regard to Intellectual Property Rights, allowing them to be freely adopted and utilised worldwide. Open standards guarantee that compliant systems will be able to work together, independent of which manufacturer provides the equipment enabling considerable economies of scale to the benefit of the industry and also the consuming public.

The DVB is market lead. Its technical specifications are written to strict commercial requirements established by consensus by its members which represent all the industry constituencies of interest and the consumer through CE and IT vendors and broadcasters who have an interest in only producing products which are compelling and affordable.

Why DVB CPCM?

In the late 1990's visionaries in the DVB predicted that the future growth of digital distribution of video and audio content; the advent of affordable consumer digital recording and processing equipment and software; and the potential for easy content movement by peer-to-peer transfer via broadband connectivity, would turn the existing consumer content usage paradigm on its head. Whilst convenient for consumers, the ease of unrestricted re-distribution of commercial content and associated loss of revenue to the content creation industry would reduce the income needed for investment in new content. The inevitable reaction of the content industry would be the push for DRM and content protection technologies in consumer products. On the other hand, a degree of content usage control, where applicable, would encourage content providers and distributors to introduce compelling new consumer propositions enhancing digital home networking and storage.

It was therefore logical that DVB should embark upon an attempt to produce a specifi-

cation for digital content protection and copy management to complement its other work in emerging new platforms. Interested DVB members determined to attempt to provide an open standard CPCM system specification for use in consumer products which, if adopted, will avoid a plethora of non-interoperable proprietary systems resulting in higher costs and consumer confusion so slowing digital take up and hindering moves towards analogue switch-over.

In September 1999 the DVB established a new commercial sub-group within its Commercial Module with a mandate to prepare Commercial Requirements for a CPCM system to provide a common framework for the protection and management of commercial content in consumer digital equipment and home networks whilst taking into account consumer interests such as; no requirement for system registration or a return path; simple to use with clearly displayed information about usage rights.

The group spent three years deriving the Commercial Requirements for CPCM which indicates the degree of difficulty in reaching consensus across the industry in the emotive area of content protection.

Inevitably viewpoints were initially somewhat polarised across the industry sectors. For example, there was clearly a need to balance the concerns of the rights owners to protect their revenues with the concerns of the consumer electronics industry to protect the investment made by their customers in purchasing equipment. Public Service broadcasters were concerned that signalling over restrictive use of their broadcast content would conflict with their public service charters. Pay TV broadcasters were looking for a means to integrate CPCM with existing Conditional Access systems to support new commercial offers such as VoD (video on demand). However, despite these differences, consensus was finally achieved by participants recognising and accommodating each other's business models.

In 2001 the Commercial Requirements for CPCM were approved by the Steering Board of the DVB and a sub group of the Technical Module was set to work to produce the specification.

The CPCM system

Although the functionality targeted for DVB-CPCM is much less ambitious than that of a full digital rights management (DRM) system, the scope envisaged is for end-to-end protection of commercial digital Content in all processes from the point of acquisition by the consumer through to the point of consumption.

Possible sources of commercial digital Content include broadcast (e.g., cable, satellite, and terrestrial), Internet-based services, packaged media, and mobile services, among others.

It is also intended that DVB-CPCM shall be applicable to the widest range of equipment encompassing in-home digital networks, personal digital recorders; in the home and portable, and facilitate remote connectivity to other locations such as a second home or a vehicle.

CPCM is intended to be used to manage all types of commercial Content – audio, video and associated applications and data delivered to consumer devices from acquisition until final consumption, or export from the CPCM system. Allowed usage is signalled by Usage State Information (USI) in the form of metadata which is securely bound to the content.

USI has been designed to accommodate a variety of business models and regulatory regimes. The existence of any particular field of USI in the specification does not imply that it will be asserted in a particular instance, or that it will be allowed to be asserted. Details regarding how and by whom a USI field can be asserted or changed will be reflected in the relevant CPCM compliance regime, which is outside the scope of the specification. For instance, European Public service broadcasters are indicating that they are considering setting a profile of CPCM USI signalling such that content scrambling should not be applied and that the only restriction required is to inhibit the re-transfer of the Content by means of the Internet.

CPCM is intended to interface with DVB Conditional Access (CA) systems and, where required, free-to-view broadcast delivery networks. It was recognised that DRM and copy protection systems already exist in the marketplace and will continue to be used and developed. Hence to the extent possible, without compromising its integrity and security, DVB-CPCM must co-exist with and interoperate with other DRM and copy protection systems.

The Authorised Domain

The DVB recognised that to conform with the traditional user experience of home recording, the portability of pre-recorded content, and expectations based on emerging digital connectivity, it was necessary to identify a mechanism to replicate the reasonable boundaries of content movement consumers have come to expect whilst not limiting the advantages of new digital technology. Based on the above, the concept of a user "Authorised Domain" was developed.

The Authorised Domain is defined as a distinguishable set of DVB CPCM compliant devices, which are owned, rented or otherwise controlled by members of a single household. A household is considered to be the social unit consisting of all individuals who live together, as occupants of the same domicile. This makes no assumptions about the physical locations of the devices owned, rented or otherwise controlled by the members of the household and no mechanisms to identify and/or authenticate the user shall be required.

A CPCM device may only be a member of one Authorised Domain at any time. When signalled by USI, Content is constrained to the Authorised Domain by which it is acquired and will not play on a devices belonging to a different Authorised Domain. However, to allow flexibility of connection a device can be re-assigned to another Authorised Domain for the purpose of consumption of Content assigned to that Domain during which time it cannot access Content which was bound to its original Authorised Domain. There is no limit to the number of times a device may move between Domains as long as the Content-to-Authorised Domain binding is maintained.

The specification provides mechanisms to determine the size and scope of the Authorised Domain; such size and scope to be decided by the implementer and possible local regulation.

DVB-CPCM can also be used to constrain Content to the local environment into which it is delivered by broadcast, if so signalled by the USI, to support local rights assigned to the broadcaster. The local restriction can be lifted after a defined period of time or the end of the transmission.

It should be emphasised again that provision of this mechanism does not mandate content distribution restriction in all cases. The USI will convey the restriction of movement within the Authorised Domain when it applies. If the restriction is not signalled by USI then the user will be allowed to send the content "outside" the Authorised Domain. It is envisaged that there will be many cases where the content owner or distributor will wish this to happen.

End-to-end protection & interoperability

A guiding principle in the development of CPCM is that implementation should not be dependant on a single technology. Rather, CPCM should provide a framework for interoperability between competing technologies. This enables a range of competing technology providers to collaborate to achieve a specification for a system which, whilst providing interoperable transfer of content between devices from a choice of providers, ensures that consumers can purchase equipment from different manufacturers in a competitive market and be assured that the equipment will inter-operate.

DVB-CPCM is intended for deployment in individual devices and in home networks. A content scrambling algorithm and secure exchange mechanism will be specified to preserve the security of the CPCM system. CPCM Content will only transfer between devices which are fully DVB-CPCM compliant, can establish mutual trust, and obey the USI. Intermediate devices, or entities such as network architecture items and storage on

hard drives or removable recordable media, should be transparent because the Content and USI is secure. This approach increases security and ease of implementation by avoiding the necessity of multiple decrypt and re-encrypt processing as would be the case if each entity, device or linkage, comprising a home network was to use incompatible security mechanisms. It also reduces the need for multiple cross-licensing.

Next steps

The DVB Technical Module sub group is working to produce the specification for the security elements, to fully technically define the characteristics of the Authorised Domain, and the means to securely bind content within its boundaries. It is hoped that these final elements of the CPCM system specification will be published by mid-2006, along with Implementation Guidelines which will give examples of the use of CPCM in a number of markets and business models. Guidance will also be provided on the scope of technical testing required to ensure interoperability and compliance.

Cross industry support

Although CPCM is probably the most contentious work item the DVB has attempted the process has received input and support from, typically 25 to 30 member companies from across the industry constituencies of interest with representation from major technology providers.

Inevitably there is likely to be criticism, even from some DVB members, of the development of any form of content protection in consumer products and accusations that DVB CPCM will limit the availability of content to consumers. But the majority of DVB members believe there is a growing market need for content protection and copy management and that the DVB history of an inclusive, open consensus building approach provides the best option for development of a specification which will provide tools with wide ranging options.

Some critics have accused the DVB of conducting this work "behind closed doors". Whilst it is true that the DVB is a member organisation, it is open to any organisation or company which wishes to participate and is willing to contribute its intellect or technology to the benefit of the industry at large. Membership requires the signing of the DVB Memorandum of Understanding which requires this commitment.

Sources

- DVB (2005): Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) System. CPCM Reference Model. DVB Document A094, November 2005; http://www.dvb.org/index.php?id=294

Acknowledgement: This significant work which started five years ago has been supported by a broad representation of DVB members from all the constituencies of interest; content providers, broadcasters, distribution platform operators, consumer product manufacturers, and technology providers. As can be imagined content protection in consumer products and some free-to-air broadcast markets is a potentially contentious issue. It has therefore taken some time to embrace the concerns of all the players in the market and for all the parties to reach a level of understanding of each other's present and future business models.

The author therefore acknowledges the work of all colleagues in the DVB commercial and technical sub-groups.

About the author: *Chris Hibbert* is Vice President Media Technologies & Standards with Walt Disney Television International. He was formerly Director of Engineering with ITV Digital in the UK during which time he became chairman of the DVB CPT group. Previously as Director of Engineering for the ITV Network he was responsible for technical strategy for DTT and was a member of the DVB group which wrote the requirements for the DVB-T specification. Hibbert is a member of the DVB Steering Board, has played an active role in the TV-Anytime Forum and is a fellow of the Royal Television Society. Contact: chris.hibbert@disney.com

Status: first posted 13/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=159

DRMTICS 2005. A truly interdisciplinary forum for DRM research. A conference report

By: Wanqing Li, Rei Safavi-Naini and Nicholas Sheppard, University of Wollongong, Wollongong, Australia

Abstract: The First International Conference on Digital Rights Management: Technology, Issues, Challenges and Systems (DRMTICS 2005) took place in Sydney from October 31 to November 2. It was the inaugural conference in an annual series covering research in all theoretical and practical aspects of digital rights management systems. The conference series serves as a broad multi-disciplinary forum for all DRM-related issues, including expression of rights, processes, methods and systems for enforcement of rights, DRM applications, together with the social, legal, usability and business aspects of DRM systems.

Keywords: conference report – copyright law, digital television, DRMS, P2P, rights expression language, technical protection measures, trusted computing

Introduction

DRMTICS 2005 (pronounced: "dramatics") was the inaugural conference in a series considering all aspects of DRM systems including issues faced by holders of digital rights who want to protect their intellectual property rights and consumers who seek to protect their privacy and to preserve their traditional pattern of access to media under existing copyright law.

The conference attracted submissions from all of Asia, Australia, Europe and North America, from which twenty-seven papers were selected for presentation at the conference. The programme also included three invited speakers and a panel session. The papers covered a variety of topics, including cryptography, digital watermarking, legal issues, rights expression languages, trusted computing and complete digital rights management frameworks.

DRMTICS 2005 was held in co-operation with IACR (International Association for Cryptologic Research; cf. sources) and the IEEE Computer Society Task Force on Information Assurance (cf. sources), and sponsors included electronics giant Motorola The full proceedings of the conference will be available in Springer's Lecture Notes in Computer Science series (DRMTICS 2006) in 2006.

Invited talks

The three invited talks were given by *Renato Iannella* (NICTA, Australia and ODRL Initiative), *Moni Naor* (Weizmann Institute of Technology, Israel) and *Karen Gettens* (Blake Dawson and Waldron, Australia).

Renato's talk focused on the evolution of rights expression languages (RELs) from the late 90's with DPRL up to Creative Commons and focusing on the ODRL REL. He looked at the standardisation of RELs and the impact this has had where successful, such as the mobile sector with the Open Mobile Alliance DRM specifications and concluded by reviewing the current "DRM Patents Saga" that has plagued the standardisation effort. He raised the issue of the applicability of some of the patents to RELs and the serious impact this will have on future research in this area, and the direct impact to systems being deployed today.

Moni surveyed some proposals for designing cryptographic schemes that take into account both human and computer abilities and weaknesses in solving various types of problems. These include schemes for traditional cryptographic tasks such as identification, authentication and encryption, as well as more modern ones, such as spam and abuse prevention, denial of service and voting.

Karen gave an overview of legal action taking place in the digital rights management world. She took us through the subtleties of the legal decisions in

- the *Sony vs Stevens* mod-chipping case in Australia;

- the *MGM vs Grokster* file-sharing network case in the United States; and
- the Universal Music vs Sharman Networks (Kazaa) case in Australia.

Karen concluded that courts have generally sought a balance between copyright owners and other parties, to the point of creating principles that are not included in the law itself. She further concluded that the particular outcomes in the file-sharing cases are very fact-specific and do not represent broad decisions for or against peer-to-peer technology.

Rights Expression Languages

A new rights expression language is being developed by the Audio Video Coding Standard Working Group of China. This was to be presented by *Ying Sha* (Chinese Academy of Sciences, China), but he was unable to travel to Australia and was represented by compatriot *Bin Zhu* (Microsoft Research Asia). *Kurt Maly* (Old Dominion University, USA) presented a comparative study of two languages not widely considered in the digital rights management literature, the eXtensible Access Control Markup Language (XACML) and the Policy Core Information Model (PCIM).

Paul Koster (Philips Research, the Netherlands) proposed to introduce "user-attributed rights" that allow users to control the way content which has been purchased is shared amongst their family, friends, etc. without interfering with the rights of the original content owner.

Legal and social aspects

Brian Fitzgerald (Queensland University of Technology, Australia) presented further details of the *Sony vs. Stevens* case. This case addresses the question of whether or not region-coding devices – such as those used in the Sony PlayStation – are to be considered "technological protection measures" under copyright. Current case law in Australia holds that they are not, but Fitzgerald warns that amendments guided by the recent Australia-US Free Trade Agreement may result in unforeseen control over the use of products being handed to multi-national corporations.

Yee Fen Lim (Macquarie University, Australia) also argued that digital rights management systems and the laws that support them increase the rights of copyright owners beyond what they are given in copyright law, to the point of creating an intellectual property regime even more powerful in some respects than that for tangible property.

Supriya Singh (Royal Melbourne Institute of Technology, Australia) and *Jenine Beekhuyzen* (Griffith University, Australia) gave an entertaining presentation disputing record companies' claims that music fans use free downloading as substitute for purchase. Their series of interviews with Australian music fans demonstrated a continuum in behaviour between free downloading and purchase: most interviewees combined freely-obtained and purchased music depending on a variety of factors including the availability of their preferred forms of music, their financial means and their level of familiarity with a particular artist.

Panel session

The panel session brought together technical and legal minds to discuss the subject *Is Reliable and Trusted DRM Realistic or Even Possible?* Discussion could no doubt continue almost indefinitely on such a provocative topic but we had to discuss what we could in an hour.

The panel was chaired by *Bill Caelli* (Queensland University of Technology, Australia). *Ezzy Dabbish* (Motorola, USA) and *Bin Zhu* (Microsoft Research Asia) presented the technical side, while the legal view was represented by *David Vaile* (Baker & Mackenzie Cyberlaw and Policy Centre, Australia), *Philip Argy* (Mallesons Stephen Jaques, Australia) and *Susanna Leisten* (Queensland University of Technology, Australia).

It seems fair to say that the general view of the technical community involved is that DRM systems will exist and their reliability and trustworthiness will be possible within certain parameters – no security system will ever be perfectly secure in itself, but it can be

secure enough to serve its purpose given the right legal and other support.

The views of legal side were less unified. While Leisten outlined the negative effects of strict regimes for protection of digital rights, Argy viewed DRM systems as a natural evolution of property protection systems. Vaile questioned the possibility of DRM systems that can provide fair use.

Cryptography

Broadcast encryption has become an important cryptographic primitive for conditional access and digital rights management systems. *Miodrag Mihaljević* (Serbian Academy of Science and Arts) presented one paper describing potential weaknesses in certain broadcast encryption schemes, and another describing a new scheme with improved efficiency and greater security than previous schemes. *Ulrich Greveler* (Ruhr University Bochum, Germany) presented a new scheme offering unconditional cryptographic security at the cost of allowing a few free-riders.

Jacques Fournier (GEMPlus S.A., France) showed how cryptographic operations can be vectorised for efficient implementation on embedded systems such as smartcards.

Tamper-resistance

The security of digital rights management systems depends on the inability of attackers to reverse-engineer and modify sensitive hardware and software components. *Mahadevan Gomathisankaran* (University of Iowa, USA) presented an architecture for verifying the correctness of systems without requiring the verifier itself to be given sensitive information about the system. *Brian Blietz* (University of Iowa, USA) presented a software tamper-resistance system based on extending the power of small, heavily-obfuscated process to a larger process that performed the real function of the software. *Valery Pryamikov* (Harper Security Consulting AS, Norway) presented a new method of preventing reverse-engineering of software based on transforming a programme's function call tree.

Watermarking

Watermarking continues to be one of the active research topics with extended applications from multimedia security to software security. *Hongmei Liu* (Sun Yat-Sen University, China) presented two papers. One is about a scheme for reversible semi-fragile image authentication that is able to locate any tampered areas but is tolerant to JPEG compression. Another is DC coefficient-based video watermarking compliant to MPEG-2 bit stream without any additional payload. *Yongwha Chung* (Korea University, Korea) presented a case using robust and fragile watermarking (dual watermarking) for the communication of fingerprints. The robust watermark may be used to identify source devices. *Clark Thomborson* (University of Auckland, New Zealand) introduced software watermarking as a means of preventing software from piracy and unauthorised modification and presented an improved version of the QP algorithm through register allocation.

Systems

The last day of the conference was mostly given over to proposals for complete digital rights management systems. *Bin Zhu* (Microsoft Research Asia, China) presented two systems, one for a privacy- and copyright-respecting peer-to-peer network and another for scaling the quality of content according to the user's willingness to pay for it. Another copyright-respecting peer-to-peer service was presented by *Kyung-Hyune Rhee* (Pukyong National University, Korea).

Ulrich Greveler (Ruhr University Bochum, Germany) discussed several methods of enforcing regional access to pay-TV broadcasts and concluded that, even though deployment of trusted hardware is considered the standard requirement for digital rights management systems, trusted hardware was not necessarily the best solution in this scenario.

Bottom line

DRMTICS provides a forum where all researchers from all disciplines with an interest in digital rights management can come together and share their views and ideas. While technical presentations decidedly out-

numbered the other presentations at this year's conference, both technical and non-technical disciplines were well-represented amongst the conference delegates. As noted in another INDICARE conference review (Kerényi 2005), a healthy exchange between the technical and non-technical communities is essential to successful deployment of digital rights management. Hopefully DRMTICS 2005 represents a good start to a significant event on the annual DRM calendar.

Sources

- DRMTICS Conference Page: http://www.titr.uow.edu.au/DRMTICS2005/
- DRMTICS (2006): Proceedings will be available in Springer's Lecture Notes in Computer Science series; http://www.springer.com/lncs
- IACR (International Association for Cryptologic Research): http://www.iacr.org
- IEEE Computer Society Task Force on Information Assurance: http://www.ieeeia.org
- Kerényi, Kristóf (2005): DRM researchers do not disregard consumer acceptability any more: http://www.indicare.org/tiki-read_article.php?articleId=157

About the author: *Rei Safavi-Naini* is a Professor in computer security at the University of Wollongong, Australia and is the Programme Chair of DRMTICS 2005 as well as the ACM Workshop on Digital Rights Management 2005. Contact: +61 2 4221 3800, rei@uow.edu.au. Wanqing Li and Nicholas Sheppard are academic staff at the University of Wollongong and are the General Co-Chairs of DRMTICS 2005. Contact: +61 2 4221 5410, wanqing@uow.edu.au and +61 2 4221 3788, nps@uow.edu.au.

Status: first posted 15/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=160

Axmedis plus = technology + users + consumers

A report on the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution (Axmedis 2005)

By: Gergely Tóth, SEARCH Laboratory, Budapest, Hungary

A report on the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution (Axmedis 2005)

Abstract: INDICARE was present at the Axmedis 2005 Conference in Florence from November 30 to December 2. The conference was organised by the Axmedis project, aiming at bringing together representatives of different fields related to cross-media. Besides the traditional scientific and industry-inspired talks, presentations focusing more or less on the consumers' point of view (e.g. interoperability or consumer protection) found their way into the programme.

Keywords: conference report – business models, collecting societies, DRMS, interoperability, privacy, standards, stakeholders, DRM users

Introduction

The Axmedis project (cf. sources) aims at reducing the cost of cross-media production and distribution, at searching for and integrating objects and components and at managing and monitoring distribution. Axmedis is an integrated project (IP), funded by the European Commission under the 6th Framework's Information Society Technologies (IST) programme, with *Paolo Nesi* from the University of Florence as its co-ordinator. Since the project specifically aims at developing and providing methods and tools for innovative and flexible Digital Rights Management, it is particularly relevant concerning INDICARE.

To fulfil its objectives the project organized the Axmedis 2005 Conference with the title *1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution* in Florence from November 30 to December 2, 2005. The three-day conference provided a rich programme. The speakers came from a wide range of organisations, thus researchers, delegates from industry, regulators and also consumer representatives were present. During the course of the conference one uncertain trend seemed to visualize for me: besides the regular scientific-, business- and industry-oriented issues, consumer-related talks could also be heard. Whether this marks the process of research and industry slowly taking the consumers' view and requirements into account or this was just the specialty of this conference and proof of the skills of the conference organisers remains to be seen.

On the first day after the welcome speeches an invited talk started the conference. Afterwards the programme continued in three or even four parallel sessions. Besides the core Axmedis subjects including an Axmedis tutorial track throughout the conference and the "Axmedis Call for take up action", there was a panel on "The role of collecting societies in the digital era" (see later), an extensive MPEG Workshop, a special session of the EUAIN project (see later) and in addition the 3rd Virtual Goods Workshop, which was co-located with the conference (see later). By this approach it was possible to address the subject matter not only from a technological point of view but from the point of users and consumers too. The whole programme is available at the homepage of the conference and all papers are available in the conference proceedings (Nesi et al. 2005).

Due to this huge programme, I was not able to attend all presentations, thus the following report will just be a subjective glimpse of the whole event. Nevertheless it has to be stated that the organisers did their best with the conference and the event progressed smoothly.

Invited talk

After the welcome talks the conference started with the invited talk by *Leonardo Chiariglione* from the DMP project (cf. Jeges and Kerényi 2005). In his talk Chiariglione argued that the protection of intellectual property should be in balance with its use. Nowadays, when analogue is shifting to digital and thus the challenge of managing scarcity is changing to managing abundance he proposed a *rational* DRM architecture, which is both scalable and interoperable and composed of standard technology and equipment.

Security of DRM

That Axmedis successfully brought together parties with different goals and backgrounds and that such presentations can form a symbiotic whole (even following up Chiariglione's vision of a rational DRM) were clearly illustrated by the next two talks given during the Content Security and Digital Rights Management session.

Josep Domingo-Ferrer presented a solution on multicast fingerprinting and collusion security. The main challenge solved was to equip multicast content with unique fingerprints, thus copy detection could be used complementary to copy prevention. This solution, which could find support in the technology domain, naturally is objectionable from the privacy (and thus the consumer's) point of view (cf. presentation by Grimm later).

On the other hand *Jose Prados* explored the possibilities of interoperability of rights expression languages (RELs) and protection mechanisms. In particular he analyzed how the REL of OMA DRM 2 (cf. sources), i.e. ODRL (cf. sources), and that of MPEG-21 (cf. sources) could be converted into each other. While the presentation focused mainly on technical issues, interoperability, i.e. to rightfully consume protected content on any device was highlighted as one of the main consumer requirements for DRM.

Collecting societies

The panel session "*The role of collecting societies in the digital era"* provided an interesting insight into the challenges these organisations face with the switch to the digital content gaining momentum in the 21st century.

Maila Sansaini from IMAIE analysed DRM from the point of view of a collecting society. While DRM can protect against privacy by applying technical measures, helping in identifying works and allowing payment for the content it still has deficiencies: current solutions are not interoperable; they do not ensure equal remuneration of copyright and neighbouring rights holders and can also be cracked.

Dominic McGonigal from PPL, UK, did not analyze DRM, he rather chose the approach of introducing the operation and problems of a collecting society to the audience. By describing the internal processes of his organisation, how the huge volume of music content is managed, how licences are stored and usage information is processed in order to distribute income between producers and performers, DRM architecture designers could gain insight into the life of a potentially important DRM system user.

Accessibility

Another session focusing mainly on the consumer was related to the interconnection of DRM and accessibility. This track was assigned to EUAIN, the European Accessible Information Network (cf. sources).

In the first talk *David Crombie* introduced the core idea behind EUAIN. He emphasized that current practice is to apply quick fixes to fill the gaps in order to achieve accessibility, while in the long term accessibility can only be achieved if it is managed as a process throughout the life-cycle of a product. This change of mind is promoted by EUAIN, and IST-funded project to promote eInclusion as a horizontal building block in the establishment of the information society.

Roger Lenoir continued by exploring the possibilities and achievements of open software and open standards as tools for accessibility. In his presentation he compared the associations representing visually impaired people with the open source communities, where in both cases voluntary work dominates. Finally, Lenoir introduced some current projects (DAISY, NIMAS, WCAG) focusing on accessibility.

Virtual Goods Workshop

This year the Virtual Goods Workshop was co-located with the Axmedis 2005 Conference. This series of workshops focuses on the multi-disciplinary assessment of existing DRM technologies and business models. Unfortunately I could not attend the whole workshop, only the first part, thus the following is a partial overview of this year's event.

In his presentation *Stephen Saunders* evaluated the current shift in the music industry from distributing music through retail stores towards the thousand-faceted digital distribution. His argument was that it was high time to start to change the way music is regarded: industry should move from thinking of music as a good to using it as a service with different service levels for different users.

Prof. Rüdiger Grimm, University of Koblenz (formerly at TU Ilmenau) introduced the results of an analysis aiming at evaluating privacy issues during DRM usage (Grimm et al. 2005). Although DRM systems' main goal is to enforce copyright, they are sometimes also used for recognition of bad behaviour, to deliver personalized watermarks and other technological methods interfering with privacy. Grimm presented results of data flow evaluations with concrete DRM architectures before completing a deal, at checkout, while checking the right during consumption, through special services and even through hidden interfaces.

Another presentation, given by *Matthias Spielkamp* from iRights.info strengthened the consumer representation at Axmedis. He introduced this German organisation which aims at delivering information about legal aspects of DRM to the consumers. The main goal is to inform the users about the legal background of typical use cases (e.g. downloading content from a peer-to-peer network or ripping a CD) in an independent way.

Bottom line

The Axmedis 2005 conference presented a good mix of research- or industry-driven and consumer-oriented talks. Although the project itself was mainly technology focused, the organisers did a great job in inviting a

broad spectrum of presenters. As an advocate of the INDICARE project who is always looking at the end-users' point of view when it comes to DRM and generally to multimedia-relates issues, I am looking forward to the next Axmedis conference in December 2006 to see whether the shift towards a more consumer-centric view will further evolve. Could it be that this conference marked the start of a larger trend? I do hope so.

Sources

- Axmedis project: http://www.axmedis.org
- Axmedis 2005 conference: http://www.axmedis.org/axmedis2005/
- Digital Media Project (2005): http://www.dmpf.org
- European Accessible Information Network: http://www.euain.org/modules/wfsection/
- Grimm, Rüdiger et al. (2005): privacy4DRM Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management: http://www.datenschutzzentrum.de/drm/privacy4drm.pdf
- iRights.info – Urheberrecht in der digitalen Welt: http://www.irights.info/
- ISO/IEC JTC1/SC29/WG11/N5231 MPEG-21 Coding of moving pictures and audio: http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm
- Jeges, Ernő and Kerényi, Kristóf (2005): Digital Media Project – Part II: Chances of an open standard. INDICARE Monitor, Vol. 2, no 6, August 2005; http://www.indicare.org/tiki-read_article.php?articleId=134
- Nesi, Paolo; Ng, Kia; Delgado, Jaime (eds.) (2005): Proceedings of the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution, IEEE Computer Society, 2005
- ODRL: http://www.odrl.org/
- Open Mobile Alliance – Digital Rights Management V2.0 Candidate Enabler: http://www.openmobilealliance.com/release_program/drm_v2_0.html

About the author

Gergely Tóth is a PhD student at the Budapest University of Technology and Economics in the SEARCH Laboratory. Besides Digital Rights Management his core interests include security and privacy. You can contact him at gergely.toth@mit.bme.hu

Status: first posted 20/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=161

Editorial of INDICARE Monitor Vol. 2, No 11, 27 Jan. 2006

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The special focus of this issue is on *DRM and accessibility*, an important topic not only for blind, partially sighted and other print disabled people. Three articles complementing one another explore the technical, legal, and policy dimensions of accessibility and present the state of the art. Further articles deal with a layered architecture for DRM, DRM in Japan's digital broadcasting services, and Sony BMG's DRM in the light of the class actions filed against the company.

Keywords: editorial – INDICARE

About this issue

DRM and accessibility

The issue's special focus is on DRM and accessibility – an important topic not only for disabled persons. This topic has already been dealt with before in the INDICARE State of the art report by *Bettina Krings* (cf. Helberger et al. 2004, pp. 30-33) and in the first supplement to this report by *Ulrich Riehm* (cf. Helberger et al. 2005, pp. 6-8).

Disabled persons, especially blind, partially sighted and other print disabled people have to rely on exemptions within copyright law allowing them to effectively use assistive technologies even in cases where the content is protected by TPMs. The three articles dealing with this subject make us aware of the troubles still existing, but also of the solutions at hand. When talking about this subject it is important to have in mind that blind and visually impaired people are consumers like you and me, and that improving accessibility is not only to the benefit of this group, but for all of us.

David Mann, who works for the Royal National Institute of the Blind in the UK and chairs the European Blind Union's Working Group on Copyright and Publishing, provides an excellent overview of the issues at stake. Among others he points to the risk that DRM might disable assistive technologies and hints at the irony that the great potential of the e-book technology, enabling the accessibility of publications as never before for print disabled people, might not be leveraged due to DRM restrictions in place. He discusses in more depth Adobe's policy in this matter presenting it as a model where access to content is granted based on trust relationships and a trusted environment. Mann also points out that the EU in its copyright directive at least – in contrast to WIPO – recognises exemptions and limitations for people with reading related disabilities. However he criticises that it falls short of providing for the harmonization of the exceptions required.

The next article stems from *David Crombie* and colleagues who are co-ordinating the European Accessible Information Network (EUAIN), a project funded by the European Commission under the 6th Framework IST programme's *eInclusion* thread. Their article puts forward two important messages:

- First, by and large technological solutions and standards required to allow print disabled people to enjoy e-content are already there (not excluding however a series of problems still around). The crucial point is that solutions developed anyway for multi-channel publishing and reuse of electronic material can also be applied for accessibility publishing. Even more, accessibility publishing may be regarded as the basis for e-content publishing in general. This turns around the logic in an important way: what is required to serve communities with special needs may change from an additional ex post activity to a prerequisite of mainstream e-content publishing.
- Second, following the authors, in order to serve disabled people, trusted intermediaries and secure environments are necessary. In more general terms this approach might suggest that all groups or communities benefiting from copyright

exceptions would have to turn into authorized consumers in trusted environments. Hence copyright legislation – allowing the application of TPMs to protect content on the one hand, while stipulating exemptions on the other hand – might imply a push for trusted computing infrastructures.

The third article of the focus theme comes from *Zoltán Nagy*, Speech Technology Ltd, Budapest. It gives an overview of the state of art of assistive technologies for the visually impaired, in particular OCR, text to speech engines (TTS), and screen readers. In terms of applications the development of e-books from simple voice books to standardized "DAISY books" is sketched. These are digital talking books combining and synchronising text and high quality voice. Many books have been published using the DAISY standard which confirms that solutions developed for print disabled have the potential to become mainstream. Another interesting service, called Világhalló, has been developed in Hungary. It is an integrated *on-line* service which combines text and voice flow to consumers, a kind of text radio. Infringing copyright is made difficult as the text alone is not accessible. This is in line with the publishers' requirements as Nagy says.

This article makes us also aware that accessibility means more for blind and visually impaired people than mere e-book text to speech transformation. There is an urgent need for *websites* designed respecting accessibility criteria, a need for assistive technology supporting the use of *software*, and a demand to make high-devices and services like *mobile phones* more accessible. Addressing these challenges, the author also hints at possible solutions.

Technical analyses

Sam Michiels, *Koen Buyens*, *Kristof Verslype*, *Wouter Joosen* and *Bart De Decker*, computer scientists from the Katholieke Universiteit Leuven, Belgium, deal with a highly relevant topic: the lack of a generic software architecture guiding the design and implementation of DRM systems or applications, and supporting interoperability of DRM technologies and their reuse. In their view software architecture design for DRM should be at the top of the research agenda. The authors propose a layered DRM architecture that supports DRM developers in producing complete and interoperable systems. The architecture is approached from both a functional and a security perspective. What makes this article particularly readable for non-techies is the fact that the authors have taken the Internet architecture as a guiding model – not disregarding however the differences when it comes to DRM. What is also very laudable is that the developers did not exclusively discuss their own solution, but relate it to the efforts of others, in this case with those of the Digital Media Project, which has been addressed in the INDICARE Monitor several times already (cf. e.g. Jeges 2005).

The second technical analysis is about Japanese digital broadcasting. We invited *Kiyohiko Ishikawa*, researcher at Japan Broadcasting Corporation (NHK), to contribute to the INDICARE Monitor, and to help us compare different approaches of content protection in different regions of the world. The author, who is currently working on a security system for digital broadcasting based on home servers, introduces us to the current state of digital broadcasting in Japan and the protection measures in place. How it works in Japan is explained in some detail. Apart from the technical details, it is interesting to see the difference between the Japanese and the US approach. In Japan, where broadcasting is scrambled but free to air, the technical protection measures applied rely on a Conditional Access System (chipcard and set-top-box), which does not need a broadcast flag.

Legal analysis of the Sony BMG rootkit scandal

Natali Helberger analyses the Sony BMG rootkit scandal from a lawyer's point of view, i.e. she goes into detail with respect to the class actions filed against Sony BMG. A class action allows e.g. consumers to complain as a group avoiding individual law suits. One of these class actions was on behalf of Sony BMG CD buyers in the US and brought by a Californian lawyer, *Alan Himmelfarb*, while the second class action was brought by the Electronic Frontier Foun-

dation (EFF) with a broader scope: against Sony BMG's XCP technology *and* the MediaMax technology used by Sony BMG, *and* provisions in the consumer contract. An important observation is that in these cases it was consumer law (and not copyright law) brought against DRM.

Sources

- Jeges, Ernő (2005): Digital Media Project – Part I. Towards an interoperable DRM platform. INDICARE Monitor, Vol. 2, Number 4, June 2005; http://www.indicare.org/tiki-read_article.php?articleId=116
- Helberger, Natali (ed.); Dufft, Nicole; Groenenboom, Margreet; Kerényi, Kristóf; Orwat, Carsten; Riehm, Ulrich (2005): Digital rights management and consumer acceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report – First supplement, Amsterdam May 2005; http://www.indicare.org/tiki-download_file.php?fileId=111
- Helberger, Natali (ed.); Dufft Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich (2004): Digital rights management and consumer acceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report, Amsterdam, December 2004; http://www.indicare.org/soareport

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 27/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=171

Digital rights management and people with sight loss

By: David Mann, European Blind Union, Lisburn, Northern Ireland.

Abstract: This article examines the barriers which digital rights management schemes can create for readers with sight loss, analyses some of the reasons for this, points to possible solutions and makes recommendations for further action by various parties.

Keywords: policy analysis – accessibility, disabled persons, e-books, EUCD, WIPO

1. Introduction

The European Blind Union (EBU) and its member organisations throughout the European Union are very concerned at the impact which digital rights management schemes can have on both blind and partially sighted people, and indeed others with a reading related disability such as dyslexia. We can be denied equal access to knowledge and culture if digital rights management schemes are inadequately designed or unfairly deployed.

Full and equitable access to information is essential if people with sight loss are to compete on equal terms in education and employment. It is also essential to full enjoyment of all aspects of daily life and of the potential advantages which modern technology brings. Voluntary agencies serving people with sight loss in member states devote significant voluntary resources to trying to ensure that blind and partially sighted people are not left behind by advances in communication, be it in the fields of broadcasting, telecommunications or publishing. This is an extremely challenging task, given the speed of development in these fields.

2. The issues for blind and partially sighted people

Blind, partially sighted and other print disabled people read electronic material by

modifying the way in which it is presented, without modifying the content. They may do this through magnification, transformation into synthetic audio, or the use of a temporary, or "refreshable" braille display. In some instances the software with which to make these changes is incorporated in mainstream packages, but the most flexible and adaptable solutions are achieved via dedicated "screen reader" software. The term "assistive technology" is used in this document to refer to this form of access.

Digital rights management schemes, or the technological protection measures within them, can react to assistive technology as if it was an illicit operation. Thus, the DRM systems applied to e-Books and e-documents can prevent access by people who use assistive technology to read the screen or to control the computer.

In those circumstances, the blind user is prevented from achieving the same degree of access as his sighted counterpart, or indeed any access at all.

A second problem can be the "disabling" of speech functions in a particular publication. While e-book readers may have the facility to reproduce synthetic speech, the rights holder can apply a level of security which prevents this from working. A person with sight loss can thus buy a book but find herself unable to read it.

We have been contacted by several people who have purchased e-Books from both major retailers and small publishers, only to find that they are unable to read them because of the way that the DRM has been applied.

For example, Lynn from London bought a Bible from Amazon, and found that the content was locked in such a way that she could not read it with her screen reader. She contacted Amazon who advised her to contact the publisher. Having taken this extraordinary step, she was told "there is nothing we can do about it".

EBU views this as discriminatory practice, as publishers are erecting barriers to access, however unwittingly. We do not believe there are commercial or technical reasons for this to continue.

This situation is in fact deeply ironic, since an e-Book can be a great way to make publications accessible to people who cannot read print. It is unsatisfactory and unnecessary because technology companies such as Adobe have actually taken steps to ensure that content can be protected and yet access still provided to disabled customers.

3. Technical analysis

Both Adobe Security and Adobe DRM can be configured to restrict the use of access tools such as screen readers. Typically, a commercial document or e-book in PDF format will have all accessibility features disabled. This is not the default position but is easily and most often selected by commercial publishers.

Microsoft e-book reader sells most of its titles with an "owner exclusive" level of security. In addition to having this "anti-piracy" function, the Owner Exclusive book also has use restrictions that apply to the legitimate owner of the e-book. In particular the text-to-speech capability that is built into Microsoft Reader for accessibility purposes is disabled. Similarly, "Owner Exclusive" limits use of the product to one device, which prevents a visually impaired user from downloading from a desk top PC to a more congenial device such as a lap top braille notetaker.

The objective of applying DRM to a piece of content is to define and implement the rules for the access to and use of that content. To achieve this, the DRM system has to operate in a controlled and trusted environment in which it is able to control all the options available to a user of the content.

This control requirement extends to accessibility tools – and explains the problems which have arisen in a conflict between DRM and accessibility. The Microsoft text to speech (TTS) synthesis tool has a broad functionality which is also incorporated in the Adobe Acrobat Reader. As a tool it is considered to pose a threat to DRM controlled content because of its broad functionality and because it does not connect in a trusted manner with the DRM system.

This is why the DRM system in the Microsoft e-Book Reader application blocks the use of the TTS tool when the DRM is configured to manage the rights in premium (commercial) content. This was originally the default position with the Adobe Reader.

There are essentially two ways in which this problem can be addressed. The first is to set up a system where the DRM mechanism is able to recognise a trusted accessibility tool and then unblock access to content for that tool. The second way is by devising instructions, expressed through the rights expression language, which are available to authorised users of trusted access tools.

Adobe has already initiated a program incorporating the first approach. The DRM system used in the Adobe reader is now able to recognise and establish a trusted relationship with at least two accessibility tools (Window-Eyes and Jaws screen readers). Allowing access to DRM protected content is now reportedly the default position of the reader.

The effect of this trusted relationship between the Reader and the accessibility tools is that access (including text to speech) can be facilitated without in any way derogating from the security level applied to the content generally (e.g. no printing, no altering, no saving to alternate formats).

To achieve this relationship, third party applications are submitted to Adobe for testing the security and compatibility issues. To quote from Adobe's *Loretta Guarino Reid*, in a response to an enquiry from the RNIB "Techies" e-mail list dated 15th December, 2005: "Our solution depends on a special mechanism that vendors can use to identify themselves as trusted clients. To implement this properly really requires suitable operating system support to provide a secure channel to trusted client programs, and a good mechanism for validating the identity of the client program."

Thus the feasibility of access to Adobe DRM through assistive technology has been established, but effective realisation remains protracted and by no means universally rolled out.

The information of this chapter is drawn largely from "Accessing and Protecting Content", by Garnett, White and Mann (Garnett et al. 2005), a report prepared during 2005 by RNIB within the European Accessible Information Network Project (cf. sources) funded by the European Commission. We would also like to recommend an article entitled "The soundproof book", by George Kerscher, International Project Manager, DAISY Consortium, and Jim Fruchterman, CEO, the Benetech Initiative (Kerscher and Fruchterman 2002). Although written some time ago, this article has not lost its validity, and still poignantly illustrates the threats posed by DRM.

4. The legal background

International treaties have long permitted national legislatures to introduce exceptions and limitations to copyright in various circumstances, including exceptions and limitations for the benefit of people with a reading related disability. By no means all EU member states yet have such exceptions, and there is no consistency amongst the exception regimes that do exist.

Unfortunately, technological protection measures can negate these exceptions if they make it difficult or impossible to access material which one is entitled to read.

At international level, the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) require, in Articles 11 and 18 respectively, legal protection for rights holders using technological protection measures. However, they make no specific provisions to protect the beneficiaries of exceptions to copyright whose access is blocked by such measures.

Individual member states and the European Union collectively will shortly be ratifying these treaties.

Fortunately, the European Copyright Directive (EUCD 2001) is more helpful. While it, too, seeks adequate safeguards for rights holders against the circumvention of technological protection measures, it does state in Article 6.4.1:

> "…in the absence of voluntary measures taken by right holders, including agreements between right holders and other parties concerned, Member States shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned" (EUCD 2001).

Article 5.3.b is the one relating to exceptions and limitations for the benefit of people with a reading related disability. Hence the Directive envisages protection against technological exclusion for such users.

Again, there is no evident consistency in the way in which these provisions are being transposed into national law. It is ironic that a directive which has the word "harmonisation" in its title does nothing to harmonise exceptions to copyright or protection of the beneficiaries of those exceptions that do exist. The EUAIN project (referred to above) will be analysing the implementation across the EU of Article 6.4.1 and, if appropriate, making recommendations to the Commission on required changes.

It is essential that governments set up robust, effective and efficient procedures to allow print disabled people who find their access blocked by a technological protection measure to gain the access to which they are entitled. For legislation to permit circumvention in certain well-defined circumstances would be helpful. That alone, however, would not be the total answer, as the potential user might not have the necessary skills to circumvent. Arrangements for prompt legal or administrative recourse are also required.

As already noted, the European Union has recognised that copyright exceptions for disabled people may be compromised by the technological protection measures within DRM Systems. Subsequent to the passage of the Directive, both DG Information Society and DG Enterprise conducted work on DRM, the latter through CEN (Centre Européen de Normalisation). This work indicated that the whole issue remains fluid and largely untested, and that interoperability and protection of consumer rights are key issues which still need to be safeguarded.

5. Conclusions and recommendations

The access rights of people with sight loss have not yet been sufficiently recognised by politicians, standards bodies, content providers or the IT industry.

Governments and Parliaments have a duty

- a) to ensure that they have comprehensive and up to date provisions to ensure that accessible copies of all published material can be created without the requirement for rights holder permission; and
- b) to establish effective measures to give the beneficiaries of such exceptions immediate and equitable access to material from which they find themselves excluded by protection or rights management measures.

If such procedures can be achieved through voluntary agreement with rights holder groups they will probably work more smoothly, but legal backing for the right of access is essential in the interests of social inclusion and equitable treatment of people with disabilities.

The publishing and IT industries also have an important role to play. The developers of DRM schemes should apply principles of universal design. They must address the impact of DRM on readers using assistive technology, ensuring that such technology is recognised as legitimate and authorising appropriate manipulation of the way in which content is presented.

It is also in publishers' interests to ensure that the way in which their assets are packaged do not limit the number of potential customers.

Sources

- European Accessible Information Network (EUAIN): http://www.euain.org
- European Blind Union (EBU): http://www.euroblind.org/
- EUCD (2001): Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf
- Garnett, N.; Mann, D.; White, M. (eds.) (2005): Accessing and protecting content. EUAIN consortium, FNB Amsterdam
- Kerscher, George; Fruchterman, Jim (2002): The soundproof book. Exploration of rights conflict and access to commercial eBooks for people with disabilities; http://www.daisy.org/publications/docs/soundproof/sound_proof_book.html
- Royal National Institute of the Blind (RNIB): http://www.rnib.org.uk/

About the author: *David Mann*, RNIB (Royal National Institute of the Blind), Chair, European Blind Union Working Group on Copyright and Publishing. David, himself visually impaired, works as a lobbyist for RNIB, the UK's leading voluntary agency for blind and partially sighted people. Previous experience includes managing the RNIB Talking Book Service and campaigning on copyright and related issues. Contact: David.Mann@rnib.org.uk

Status: first posted 26/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=170

Trusted intermediaries are key to accessible content delivery

By: Crombie, D., Lenoir, R., Mann, D., and McKenzie, N., EUAIN Network, Amsterdam, The Netherlands

Abstract: Much of the discussion around DRM and Accessibility has necessarily focused on the right of access versus the need to protect content. However, points of common interest exist and the development of *trusted intermediary* concepts can offer real-world solutions. The EUAIN network seeks to balance the needs of publishers and content providers with specialist organisations providing alternative format materials.

Keywords: policy analysis – accessibility, disabled persons, inclusion, intermediaries, publishing, trusted third party

Introduction

The European Accessible Information Network is a community of organisations and individuals who are examining new approaches to accessible content processing. The EUAIN network is funded by the *eInclusion* thread of the European Commission 6th Framework IST programme and is co-ordinated by FNB Netherlands (for recent publications cf. sources).

EUAIN brings together the different actors in the content creation and publishing industries around a common set of objectives relating to the provision of accessible information. Accessibility for print impaired people can be an increasingly integrated component of the document management and publishing process and should not be a specialised, additional service. Print impaired here refers to people who are blind, visually impaired or dyslexic. EUAIN takes the broadest definition of content creators and provides the support, tools and expertise to enable them to provide accessible information.

This article outlines the role of trusted intermediaries in accessible content processing workflows, giving examples of successful collaboration between content providers and specialist organisations. The regulatory chal-

lenges are also mentioned as are a number of technical and organisational considerations.

Technology and standards to serve groups with special needs are at hand

From a technical perspective, earlier problems relating to the digitisation of materials have been largely overcome and recent formats (such as XML, RDF, METS, MARC21 etc) provide a realistic basis for implementing the different aspects of this work. It is now possible to address the key concerns of content creators and providers and coherently to address issues such as: automation of document structuring, adherence to emerging standards, workflow support, digital rights management and secure distribution platforms.

For example, the recent Forrester Research report which foresaw publishers changing current business practices to match the internet's speed and convenience with the multichannel publishing model is now finding some practical application, which can offer greater consumer choice, variable presentations and delivery which is of crucial importance for those who require alternative formats. In Austria, it has been found that when publishers consider accessibility, their data can be re-used several times for multichannel publishing. As the lifetime of a book gets shorter and shorter, publishers frequently have to offer access to digital versions of that book and taking this into account when constructing the layout brings us much closer to real accessibility in the wider sense. Indeed, it has been the accessibility community that has in many ways pioneered new structures for digital content, as these developments are often borne of need. The recent EUAIN Workshop on Generating Structures examined these developments across Europe and the report is now available.

Similarly, emerging international and European standards provide an excellent basis for the creation of accessible information at a more fundamental level than has previously been possible. Whereas many earlier solutions have been at a 'workaround' level, with an accessibility component added at the end of the content creation process (if at all), it is now possible to see DAISY 3.0/NISO z39.86 as the de facto XML standard which can allow content creators significantly to enlarge their markets through the adoption of this inclusive format (cf. sources). Indeed, the navigational possibilities afforded by DAISY 3.0 are thus available to everyone, and not solely to those people who are print impaired.

At a European and national level, there now exists a clear desire on the part of publishers and associations of publishers to collaborate closely with experts in this area in order to provide truly accessible materials. Indeed, in several countries recent legislation has added an extra push to these concerns. This convergence at a technical, regulatory and political level means that the pieces of the jigsaw are now in place to make a significant breakthrough in the provision of accessible information within secure environments.

Trusted intermediaries and secure environments

Trusted intermediaries establish a personalised relationship between content holders and specialist organisations whereby publishers and agencies serving blind and partially sighted people work together in a secure and trusting environment to increase the quantity and timeliness of titles available in an accessible format. Within trusted intermediary frameworks, DRM is an enabler of controlled access. A number of different security methods are being developed or are already in use for making content available in this way.

As far as security is concerned, the higher the level the more likely publishers are to allow content to be made available in accessible digital formats. At present, the security systems used are simple, they use basic encryption technologies with key exchange mechanisms. The potential for the release of content is considerable – although there are few recorded instances of such occurring. Once decrypted, content is available to anyone, authorised or not. The ability to attach content to particular devices, or better to provide access only to authorised users, requires a level of DRM sophistication that is not yet generally in place in services catering to the needs of visually impaired people.

By way of illustration, in Belgium the national newspapers De Standaard and Het Nieuwsblad are offered in an electronic version (DiGiKrant) and a Braille paper version (BrailleKrant). This is achieved through means of a trusted intermediary. By placing a small specialist team within the newspaper publisher's offices, the alternative versions of the newspapers can be produced at the same time as the standard newsprint. Other solutions involve the news content being edited by external specialist organisations using online delivery mechanisms or delivery on CD-ROM.

In the Netherlands, an agreement was reached with the Dutch Publishers Association (Nederlands Uitgeversverbond) and the specialist organisation FNB whereby a small fee is paid for each title that is transformed into an accessible format. In addition, publishers have agreed to allow access to digital source files where feasible. This approach is an excellent example of an organisation (FNB) operating as a trusted intermediary and ensuring that the output materials are only given to registered end-users across secure distribution platforms.

In France, BrailleNet (cf. sources) has established contracts with more than 80 publishers and with an organisation managing the rights on behalf of publishers and this is the contractual basis of the Helene Server. Organisations that have been certified get an authorisation for a secured access to source files. The server Hélène contains both literary and school books in French and publishers who have contracted with BrailleNet provide the files. In the UK, RNIB has good working relations with several publishers and has been developing the *trusted intermediary* concept, and one collaborator is one of the world's largest publishers.

Challenges ahead

DRM solutions prevent content from being accessed by any person that has not been authorised to do so. This protection can happen at different levels, ranging from opening and reading the document to copying and transforming it. Agencies producing materials in alternative formats to serve persons with disabilities need to access content in order to transform it into formats that are suitable for those who cannot read it in the way it has been originally produced. Naturally these considerations also apply within mainstream publishing workflows where accessibility can also be incorporated.

The European Directive on Copyright (2001/29/EC) expresses the right to access content without any technological protection measures when the exemption for persons with disabilities has been adopted by the national legislation but at the time of writing this EC Directive has been implemented in a variety of different ways. WIPO has also recently included similar exemptions as a recommendation to those countries in the process of setting up copyright legislation. A further problem related with copyright and intellectual property rights has to do with trans-national interchange of materials. Some copyright legislations allow only for the use and transformation of documents within the boundaries of the country where it has been originally produced, which automatically eliminates the possibility of making it available to persons with the same needs, sharing sometimes the same language, in a different part of the world. The World Blind Union (WBU), IFLA Libraries for the Blind Section and WIPO have recently initiated a survey to examine the barriers to international transfer of accessible materials in order to draw conclusions and to make recommendations on any need for changes to national laws or international treaties received the support of many countries.

Alongside these regulatory challenges, a number of technical and organisational challenges are also relevant. In this sense we must see accessibility itself as a process and not a product, a characteristic shared by DRM systems. When considering notions of access, four further issues are noteworthy:

- access to structured digital formats

Currently there are many digital formats that are inaccessible to persons with disabilities even through adaptive technology. Those formats that are based mainly on images that are not described properly are very difficult to access. Very little attention is paid to structuring information through tagging.

Documents that use tags for describing the different elements in their structure (like XHTML or XML) are of great use for those agencies producing accessible materials. Emerging multimedia formats offer opportunities to embrace accessibility issues, especially when they're based in highly structured formats and MPEG is particularly important in this respect. Within MPEG modelling environments, interfacing between Accessibility and DRM objects is highly feasible.

- access when and where it is needed

When information has to undergo complicated and costly adaptation post-processes before becoming truly accessible, the delay in getting access to that information can be excessive. Access to information in digital formats allows for easy and fast distribution to anybody at any time. The distribution of source files in a format that can be easily translated into other accessible formats allows also for customization of the information before being finally delivered to the user in the required format. Just-in-time distribution (as opposed to Just-in-case storage where everything is digitised) would actually help in making information accessible in a more efficient way.

- access to source materials

Accessing materials at source prevents agencies from spending resources on re-digitising final products. This saves time and resources in giving services to those who cannot read printed materials. If that source material is provided in a format that is already prepared for further transformation and in an agreed standard form, the time and resources saved will be even bigger. However, content providers are usually reluctant to provide publishers of materials in alternative formats with their digital masters. Fear of piracy and the evident ease in which this happens in the digital world are usually the main reasons given by publishers. As noted above, agreements with publishers in which these agencies are seen as *trusted intermediaries* seem to be the most viable solution to this situation.

- access to consistent content

Publishers of accessible materials are aware of the importance of creating consistent content. Their function is to make content accessible, the same content that is available for persons without disabilities, without altering it, without adding to or taking any information away from the original, except where extra information is needed to describe what cannot be made accessible otherwise (pictures, charts, graphics, etc.). It is important for content providers (e.g. medicine labelling) that correct and approved information is used and nothing is lost during the transformation process. Using the information provided directly by the original publisher helps in guaranteeing this. It is also important for the impaired user that no information is lost, so that the content they can access is exactly the same as that originally published. Greater co-operation is required between EU countries to avoid duplication of effort and expense as separate national practices prevent from interchanging materials that are already available in other countries.

Bottom line

It can be seen that the choice of appropriate technical protection measures for making content accessible is not straightforward and involves different considerations. The *trusted intermediary* approach has provided concrete examples of successful collaboration. Where appropriate, light DRM solutions have been applied. Further research is required to examine accessibility in the wider sense and to examine the requirements for modelling accessibility and DRM within emerging multimedia environments.

Sources

- Crombie, D (ed) (2005): Generating structures , EUAIN Consortium, Amsterdam; http://www.euain.org/modules/wfsection/article.php?articleid=161
- Crombie, David; Lenoir, Roger; McKenzie, Neil (2005): Towards accessible content management systems, ELPUB2005, Leuven Belgium, see http://anderslezen.nl
- DAISY Consortium: http://www.daisy.org

- du Bourguet, Guillaume; Guillon, Benoit; Burger, Dominique (2003): Helene: a collaborative server to create and securely deliver documents for the blind. Proceedings AAATE 2003, see http://serveur-helene.org
- European Accessible Information Network (EUAIN): http://www.euain.org
- Forrester Research (2000): Books Unbound, http://www.forrester.com/ER/Press/Release/0,1769,470,FF.html
- Garnett, N., Mann, D. & White, M., (eds) (2005): Accessing & protecting content, EUAIN Consortium, FNB, Amsterdam
- Standing Committee on Copyrights of WIPO, 21-23 November 2005

About the authors: The authors co-ordinate the EUAIN network for FNB (NL) and RNIB (UK). *David Crombie* is head of the FNB International Projects department in Amsterdam, alongside researchers *Roger Lenoir* and *Neil McKenzie*. The team has been active in many EC funded research projects over the last ten years, in particular relating to *eInclusion*, Cultural Heritage and Digital Libraries. *David Mann* is a Campaigns Officer for RNIB, and has focussed in particular on copyright issues and on the Right to Read campaign. As well as working at national level, he has been active in developing links with the World Intellectual Property Organisation (WIPO) and the International Publishers Association. Contact: nmackenzie@fnb.nl

Status: first posted 26/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=169

Digital rights management and accessibility

By: Zoltán Nagy, Speech Technology Ltd, Budapest, Hungary

Abstract: The article addresses accessibility issues for blind and visually impaired consumers. Technical tools like OCR, text to speech engines, and screen readers are introduced. Limitations of these tools as well as new promising approaches are discussed. Finally attention is drawn to the problems disabled people face when using websites, software, and mobile phones.

Keywords: technical analysis – accessibility, consumer expectations, disabled persons, e-books

Introduction

An everyday story

On an average summer day Mr. Smith, an average visually impaired man, goes into an average library to try to read an average monthly. He goes to a computer and realizes there is no screen reader installed – a screen reader is a software application that attempts to identify and interpret what is being displayed on the screen. No problem he thinks, he goes home and takes his notebook with a screen reader to the library. However the employees of the library refuse this solution suspecting Mr. Smith might be going to launch a publishing company. So he asks the librarians to scan the article he is interested in so that he can read it out with his own computer at home. This does not work either, because the librarians are not allowed to let anything leave the institution in electronic form. Eventually Mr. Smith goes back home with a single copy of the article in print. This situation is neither satisfying nor transparent for both actors: the visually disabled and the librarians.

Visually impaired persons are consumers like you and me

In the European Union there are more than 10 million people who have significant sight loss and are not likely to be able to read printed news. Since average life expectancy is continuously rising, more and more people have impaired sight. These people do not identify themselves as blind or partially sighted, but they are only able to read published materials by using alternative methods.

We have no exact statistical figure about the number of people suffering from dyslexia or about the state of their disability, but according to experts about 4% of the population is severely dyslexic. A further 6% have mild to moderate problems.

Naturally some aspects of the lives of blind people are significantly different from average people, but considering the consumption of (digital) contents they are not different at all. They listen to radio and television, they usually have CD and/or DVD players and they buy films. They are up-to-date with regard to movies, celebrities and series like anybody else. These offerings are essential for them to be full members of society.

In this article we try to give an overview of the technologies which assist the visually impaired in being consumers and users of content, and the accessibility problems they face. It also outlines a solution to some of the problems.

Technology: TTS and screen readers

To use a computer a blind person needs a text to speech engine (TTS) that can read texts out. TTS is responsible for speaking but not what to speak. Under Windows operating systems TTS engines usually support Ms Speech API – which is the standard way to create speaking enabled applications.

A screen reader is a special application which can narrate applications, or screen, or system and keyboard events. It echoes keypresses, appearance of windows and message boxes (even system bubbles of XP). Screen readers do not use OCR techniques. Optical character recognition involves computer software designed to translate images of typewritten text (usually captured by a scanner) into machine-editable text. Screen reader applications are based on special programming techniques, so called hooking, and a lot of heuristics and scripts. Usually it contains a special display driver, which tries to catch/capture the text printing function calls. This application interprets the screen for the blind and speaks out every message by a TTS engine.

There is a small group of applications which are developed for the blind: usually special blind games or learning environments or web browsers. Such software can be used by the blind without any screen reader application. The user interface of these applications is designed for the special requirements of blind users.

Limits and problems of screen readers

The first screen readers applied hooking mechanism (under Windows), but as time went on they became more and more complicated and it got more and more difficult to get textual information off the screen. Some applications even deliberately prevented other applications from getting text from that application. A wide known example is the Adobe Acrobat Reader in its earlier versions.

Furthermore, screen reader software is unable to read textual documents appearing in the windows of that application. This phenomenon is typical for applications which have their own text drawing function. To solve this problem companies like Adobe offer accessibility packs on their websites. After installing such a pack it is possible to read the document aloud from the menu. Later versions (6.0 and later) of Adobe Acrobat Reader have incorporated that function directly. The functionality however is quite poor, because only individual pages or full documents can be read aloud. An up-to-date screen reader software should be able to read out text parts of different sizes (page, paragraph, sentence, word and letters too)!

Microsoft specified the IAccessibility interface as a standard way to give information to screen readers. Unfortunately, this interface is supported by only few applications, because its implementation would mean a lot of "unnecessary" additional effort.

As a matter of piquancy, different by-passes – like the one used by Adobe Acrobat Reader – do not guarantee to prevent getting content. A professional software developer can develop a fake TTS with just 15 minutes' work, which instead of reading the text aloud collects it in a file. This manoeuvre can be performed with the IAccessibility interface too. However, as the user interface does not allow reading complete documents aloud

contiguously but just in small pieces, this type of attack is made difficult here.

From simple voice books to DAISY books

A printed book is available to a blind person by scanning, then transforming the text with the help of OCR software into digital text and reading it out by a screen reader. This long and complicated task can be performed by a blind person after practicing it for a while provided he or she has the needed equipment. We can imagine what an overhead of work this means for each blind person to scan the same book. In practice, blind people share books scanned and transformed into speech, and blind peoples' organisations collect these materials, tolerated by copyright owners. Some countries allow copying books in that way for people with disabilities provided it is not for profit. Copyright owners tolerate this. However, publishers are more and more afraid, and not without ground, that books digitised in that way can easily be shared via file sharing applications. To digitise a book is hard work. Average users will not start to scan and recognise (by OCR) a hundred-page long book, but if he or she has ready access, that's quite a different story.

In the beginning voice books were recordings available on different media. Then, with the spread of computers they appeared in more and more sophisticated forms. The length of audio files on a single CD was increased by compression. Hybrid talking books also appeared which contained the book in text and in voice form as well making the content capable for key word searching. Talking books are not only for people with disabilities. The value of a literary work can be increased if it is performed by a well know actor.

In this context the DAISY standard is very important. The DAISY Consortium was formed in May 1996 by talking book libraries to lead the worldwide transition from analogue to digital talking books. DAISY denotes the Digital Accessible Information SYstem which is the standard, when we talk about books made for visually impaired. This is a very widespread format used all over the world from the USA to Japan. The secret of the success of DAISY is that it uses a simple open format. Not only player software and devices but various types of DAISY editors are available. Many of them can be used by the blind, so organisations of the visually impaired can make their own talking books. DAISY digital talking books contain the text in XML format plus the high quality voice record synchronised with the text. DAISY books are distributed on CD-ROMs and there are many portable players. DAISY does not make possible either the encryption of information or the identification of users, which is a limitation in terms of DRM, because it relies on these two components. For more details see the DAISY standard; cf. sources). However, many books are published in that form worldwide not only for people with disabilities.

An innovative solution from Hungary

There are solutions which aim to take everybodys' interests into consideration. "Világhalló" is a Hungarian service supported by Hungarian publishers which started in 1999. Világhalló is an integrated on-line service which forwards available texts as a combined text and voice flow to the user (as a text radio) using special voice-text synchronised protocol (wow) developed specially for this purpose. By the way, "Világhalló" is a play on words which converts the Hungarian name of the Internet to "World Listener". Copyrighted content is stored on a secure server and a client program downloads the voice. This solution has an advantage regarding copyright, because the text alone is not accessible by the user. This is in line with the publishers' requirements.

"Világhalló" deals with stored text, irrespective of its genuine format (HTML, ZIPHTML, TXT, ZIPTXT, MSWORD, RTF, XML, SGML) and transforms it into a format for best reading aloud. The software adds to the text informative, structural annotations concerning the reading aloud (like sentence, paragraph, strophe, chapter, etc. or foreign word pronunciation even in inflected form).

This system is mostly used by the blind, since it is not really suitable for everyday people. Publishers make some of their copy-

righted products available to gain experience. In the early phases of Világhalló it had no users at all, because accessing the content needed continuous broadband Internet access, which meant high cost, especially for the blind. During the last six years, the service has overcome the first difficulties, and now it has 16.000 users. What is more, it has managed to get the full trust of publishers and within a few weeks works published by Magvető, one of the leading Hungarian publishing companies, will become available on Világhalló.

Accessibility issues beyond books

Problems using websites

Questions connected to persons with disabilities are not always technological. Many publicly available free contents are not accessible for visually impaired people, because the content is visually organised in such a way that without seeing it, the text turns into an unembraceable continuum. An excellent example for this is an average news portal. The structure of pages targets the majority of visitors. To make such a portal readable for visually impaired people we have to make many simplifications. Fortunately, contents are stored in databases by up-to-date portal engines so a blind friendly version can easily be produced simultaneously with the normal appearance. Governments could motivate companies to work on these developments by subsidised tenders. In the ideal case, this would even provide work for people with disabilities to be involved not only in testing but in development too.

Problems using software

Access to content is difficult for the visually impaired, but so is the use of software. I do not mean here sophisticated programs like a video editor, but the most essential programs. Many software user interfaces use exotic or mouse optimised controls which can not be handled by screen readers. That would not mean a problem itself if the impaired could choose an alternative solution, another software. The trouble however is, that this phenomena often occurs even in developments targeting visually impaired people! Although there is an ergonomic standard for such applications, many developments don't take it into account. This situation could be avoided if someone really concerned were to work in a developer team, and if the opinions of people concerned were collected in the design phase.

Problems using high-tech gadgets

Most music players use LCD displays to display textual information. This is totally unusable for a visually impaired person. However, many blind people use such equipment, simply memorising the menus and the order of the buttons. Many of the blind, using the same method, are able to even send SMS. The use of mobile phones is one of the challenges facing the vision-impaired. Mobile phones are designed primarily on visual concepts, without considering the needs of the blind or partially sighted. There are some screen reader solutions for mobile phones that allow access to most of the functionality of the device. These are designed to work with the Symbian-based operating system (mostly business class Nokia and some Ericsson, Samsung, Panasonic and Siemens phones). These products allow access to all of the phone's applications, including third-party applications.

Bottom line

The biggest accessibility problem today is that publishers and copyright owners are not, or not really, interested in serving the blind or people suffering from dyslexia. If there were a standard system which ensured copy protection and made content available in digital form, the visually impaired would become a valuable market for publishers.

Sources:

- American Library Association (2005): Digital Rights Management and Accessibility; http://www.ala.org/ala/washoff/oitp/emailtutorials/accessibilitya/10.htm
- Anderson, Ross (2003): Trusted Computing Frequently Asked Questions (Version 1.1 (August 2003); http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
- Clark, Joe (2003): Accessibility implications of digital rights management; http://www.joeclark.org/access/resources/DRM.html

- DAISY: http://www.daisy.org (The DAISY Consortium was formed in May, 1996 by talking book libraries to lead the worldwide transition from analogue to Digital Talking Books. DAISY denotes the Digital Accessible Information System).
- Kerscher, George; Kawamura, Hiroshi (2001): DRM for persons who are blind AND/OR print disabled; http://www.w3.org/2000/12/drm-ws/pp/daisy.html
- Világhalló portal – Online Reading System: http://www.vilaghallo.hu/english.html

About the author: *Zoltán Nagy* is the Head of Development at Speech Technology Ltd. which develops speech processing solutions and has taken part in many projects aiming visually impaired users. For more information see: http://www.speect.com

Status: first posted 26/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=168

DRM interoperability and reusability through a generic software architecture

By: Sam Michiels, Koen Buyens, Kristof Verslype, Wouter Joosen and Bart De Decker,
Dept. of Computer Science, K.U.Leuven, Leuven, Belgium

Abstract: The domain of digital rights management (DRM) is currently lacking a generic software architecture that supports interoperability between and reuse of specific DRM technologies. This lack of architectural support is a serious drawback in light of the rapid evolution of a complex domain like DRM. It is highly unlikely that a single DRM technology will be able to support the diversity of devices, users, and media, not to mention the wide variety of requirements concerning security, flexibility, and efficiency.

Keywords: technical analysis – DRMS, interoperability, software architectures

Challenges to DRM development

Systems that provide digital rights management (DRM) are highly complex and extensive: DRM technologies must support a diversity of devices, users, platforms, and media, and a wide variety of system requirements concerning security, flexibility, and manageability. This complexity and extensiveness poses three major challenges to DRM development, which provide the context of this article: fragmentation of individual solutions, limited reuse of and interoperability between DRM systems, and lack of a DRM software architecture that supports and guides the design and implementation of DRM systems and their applications.

- The first challenge relates to the fact that state-of-the-art DRM technologies are often ad-hoc, which leads to fragmented DRM solutions (e.g. for music, for pictures, or for digital TV) and makes it very difficult to complete the complex and extensive DRM picture.
- The second challenge, limited reuse and interoperability, is partly caused by in-house developed solutions that are incompatible with similar systems produced by other parties. Currently, for instance, an access service implemented by Apple cannot easily be reused in a Microsoft DRM system, even if both parties would like to do so. Although various DRM developers have produced "vertically integrated" designs in which their particular set of components are specifically conceived to collaborate, their solutions are unable to interoperate with components from other groups. Given the complexity and extensiveness of DRM, interoperability between specific DRM services is crucial to allow (small scale) projects to contribute to the development of particular DRM services (Jamkhedkar and Heileman, 2004).
- The third challenge, lack of a DRM software architecture, is typical for complex

software systems in evolution, and providing a software architecture is often a sign of growing maturity of the application domain. A software architecture can be seen as a generic structure that identifies the main service components and shows how they can interact. Having available such generic structure helps to evolve towards a complete set of interoperable DRM service components.

The challenges of integrating independent service components are well-recognized and are being addressed in other application domains than DRM, such as network communication, web services, or graphical user interfaces. The Internet architecture, for instance, convincingly demonstrates how a properly chosen software architecture can shape the evolution of a complex system across vast changes in technology, scale, and usage. The power of the Internet lies not so much in the elegance or efficiency of its individual components, but in the overall ability to encompass tremendous growth in scale and diversity as usage and technology continue to evolve.

A layered DRM architecture as solution

This article describes an academic study that argues for a layered DRM architecture that supports DRM developers in producing complete and interoperable systems (Michiels et al., 2005). The architecture is approached from both a functional and a security perspective. The functional perspective zooms in on the top layers, closest to the applications using the architecture. The security perspective focuses on the bottom layers, which offer cryptographic primitives to enforce digital rights. In other words, the cryptographic primitives at the bottom layers lay the foundation for the upper layers to build upon. Finally, the proposed architecture is validated by matching it to state-of-the-art DRM technologies.

Our study presents a layered architecture and identifies the key DRM services of each layer. The main contribution of this study is that it presents a next step towards a software architecture that supports reuse and cooperation of multiple domain-specific DRM technologies and standards. It is our belief that this architecture lays the foundation for addressing the above-mentioned challenges of fragmentation, reusability and interoperability, and guides developers of DRM software systems and applications in the right direction.

The proposed architecture in a nutshell

The study presents the main system requirements from three application viewpoints: the content consumer's, the content producer's, and the content publisher's. In addition, it identifies for each viewpoint the core functional services that are needed in a complete DRM system to provide this application-level functionality. In this way, seven key DRM services have been identified (see Figure 1): the Content Service (e.g. search for content), the License Service (e.g. issue licenses), the Access Service (e.g. authenticate consumers), the Tracking Service (e.g. produce usage statistics), the Payment Service (e.g. billing), the Import Service (e.g. submit content to the DRM system), and the Identification Service (e.g. reveal abusers). Next to functional services, the study identifies the hot spots in this architecture that require specific security services (such as authentication, confidentiality, and anonymity), and the cryptographic primitives needed to implement them (e.g. watermarks, digital signatures, certificates, and encryption). Remark that a single security service can be implemented by multiple cryptographic primitives depending on the requirements. For example, user authentication can be implemented by using digital signatures; yet, if user anonymity is required as well, other techniques such as zero-knowledge proofs must be used instead. The functional and security services are combined and presented in an architectural overview as shown in Figure 1. The model consists of a distributed view and perspectives from the side of the consumer, the producer, and the publisher, a layered architecture for each party, and identification of components in each layer.

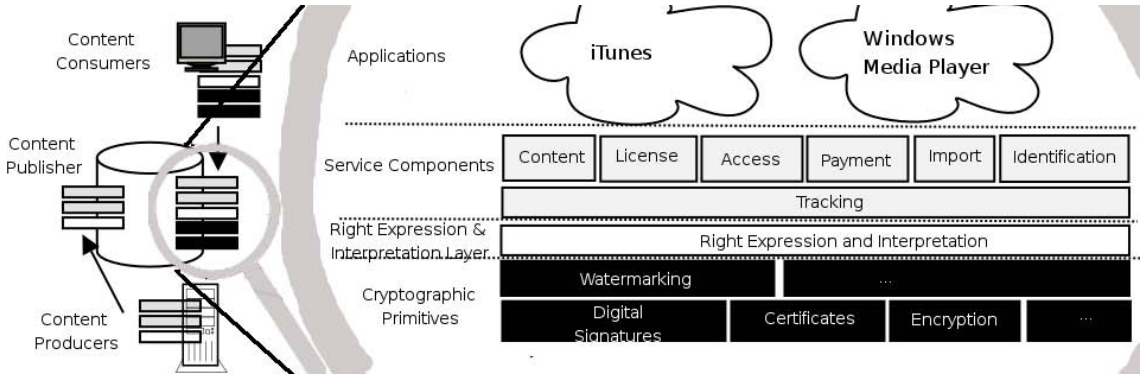


Figure 1: A distributed view on an architecture for DRM with a content consumer, producer, and publisher. The figure zooms in on the layered architecture of the publisher

Validation of the approach

By way of validation of the proposed approach, the study maps state-of-the-art DRM technologies onto the architecture and discusses how it supports the three main challenges formulated earlier. The validation is based on six DRM technologies on which technical information was publicly available: Windows Media DRM, Lightweight DRM, EMMS, Helix DRM, Aegis DRM, and the OMA specification.

Table 1: Overview of provided services of state-of-the-art DRM technologies.

DRM tech/ Service	Content	License	Access	Tracking	Payment	Import	Identification
WMDRM	X	X	-	X	-	X	-
LWDRM	X	-	X	-	X	-	-
EMMS	X	X	X	X	X	X	-
Helix	X	X	X	X	-	-	-
Aegis	-	X	X	X	-	-	-
OMA	X	X	X	-	X	-	-

As the overview in Table 1 shows, some services are provided almost uniformly by all technologies, while others are only offered sporadically. The Content and License Services are almost always implemented, which seems nothing but normal for such key services. Services for accessing, tracking, paying and importing are provided in approximately 50% of the cases, while the Identification Service is not implemented by any of the studied DRM techniques, at least not to our knowledge.

When relating these results with the three main DRM challenges presented in the introduction (completeness, interoperability, and software architecture support) we can draw the following conclusions.

- First of all, the fact that so many different DRM technologies implement the same or similar services confirms our claim that we need an architecture that promotes reuse of and interoperation between individual service components.
- Secondly, the study shows that the services with the highest benefit from reuse and interoperation are the Content and License Service. All DRM technologies that need these services would benefit from a reusable implementation.

- Thirdly, since judging from the study different DRM technologies implement different sets of services, trying to standardize 'the' DRM technology seems less efficient than focusing on particular services these technologies are composed of.

DRM architecture and Internet architecture compared

This brings us back to the analogy with the Internet architecture, which clearly identifies service responsibilities and a common platform that can support a wide variety of networking services. This architecture proves that a complete solution can be offered by a single platform if it allows reusable services to be plugged in, without trying to provide a single overall standard implementation. In other words, although service implementations may vary (for example, the access service implementation on a mobile phone will clearly be totally different from a version for a desktop computer), the architecture in which a service component is embedded and the interfaces it provides to other service is always the same. Until today, many different companies and organizations extend the TCP/IP architecture with protocols for quality-of-service, wireless communication, media streaming, or security. If we are to provide complete DRM solutions, following the Internet approach seems to be a good idea.

However, we should be aware that the Internet approach cannot be adopted as such in the domain of DRM. Although the idea of using a layered architecture for DRM solutions looks very promising, we have to be aware that the match between TCP/IP and DRM is not complete for two reasons. First of all, the DRM architecture does not completely adhere to a layered structure. This is especially true when looking at the architecture from the perspective of adaptability and manageability, two crucial quality attributes for DRM systems, which often have to be tuned to various business policies or local legislations. Such concerns can turn the main advantage of layering, i.e. virtualization of lower layer details, into a major disadvantage. This situation occurs, for instance, when lower layers do not behave exactly as required by upper layers or applications. In this case, applications should be able to fine-tune the underlying system by injecting specific policies. This is a generic problem that has already been explored in other application domains than DRM.

The second reason to be careful when comparing TCP/IP and DRM is that the architecture of the latter will not always be symmetric: while a TCP/IP client runs exactly the same protocols as the server, this is not necessarily the case for DRM systems. The right expression layer, for instance, will probably be fully implemented on the publisher's side to allow for content producers to associate with their content a wide variety of business policies. Yet, from a content consumer's perspective, this layer will typically be minimally implemented to prevent clients from tampering with business policies. The same is true for rights enforcement technologies such as watermarking, digital signatures, or certificates.

DRM Architecture and DMP compared

The Digital Media Project (DMP web site, 2005) proposes a similar approach to increase interoperability of DRM services. It defines users (e.g. consumers, producers, or publishers) as entities that perform so-called *primitive functions,* which represent the underlying DRM services that handle digital content. The primitive functions can be related to the functionality of the service components (e.g. revoke user), the rights expression and interpretation layer (e.g. represent rights expression), or the security components (e.g. represent key). The DRM architecture we have presented structures the domain by locating the set of primitive functions (components) in three layers: the service components layer, the rights expression and interpretation layer, and the security layer. Both approaches focus on interoperability by providing functions (components) with well-defined responsibilities.

Bottom Line

The presented model has confirmed the potential benefits of applying software architectures to inventory, analyze, and discuss research in this field, and has proven to be

useful to set the agenda for the future. If DRM is not to end as the umpteenth flash in the data protection pan, it may be high time to put software architecture design at the top of its research agenda. In our opinion, the next steps to be taken in this research field are (1) to refine the interaction interfaces of the identified service components, and (2) to apply and validate the proposed architecture in a case study to reveal additional issues driven by non-functional requirements (e.g. efficiency of content distribution, content personalization, or context awareness).

Sources

- The Digital Media Project (DMP) web site (2005): http://www.dmpf.org
- Jamkhedkar, Pramod; Heileman, Gregory (2004): DRM as a Layered System. In: Feigenbaum, Joan; Sander, Thomas; Yung, Moti (Eds.) Proceedings of the 4th ACM workshop on Digital Rights Management (DRM'04), Washington, DC, USA. ACM Press, pp. 11–21
- Michiels, Sam; Verslype, Kristof; Joosen, Wouter; De Decker, Bart (2005): Towards a Software Architecture for DRM. In: Safavi-Naini, Rei; Yung, Moti, (Eds.): Proceedings of the 5th ACM Workshop on Digital Rights Management (DRM'05), Alexandria, VA, USA. ACM Press, pp. 65-74

Acknowledgements: This article is a summary of (Michiels et al., 2005) and presents a study which brings us one step closer to a generic software architecture for DRM. Research for this article is part of the E-PAPER project, funded by the Interdisciplinary institute for BroadBand Technology (IBBT). The project is being carried out in collaboration with a consortium of companies: Philips, De Tijd, Belgacom, Hypervision and I-Merge. The authors are very grateful to Ann Heylighen for her valuable comments and for proof reading the text.

About the authors: *Sam Michiels* is a postdoc researcher at the Computer Science Department of the K.U.Leuven. He received his Ph.D. in computer science in 2003. His main interests include software technology and network middleware. *Koen Buyens* is a researcher in the Computer Science Department of the K.U.Leuven. His main interests include secure development of applications and middleware. *Kristof Verslype* is a Ph.D. student at the Computer Science Department of the K.U.Leuven. His main interests include secure software and anonymity. *Wouter Joosen* is professor at the computer science department of the K.U.Leuven. His research interests include software architectures for distributed systems, aspect-oriented and component-based software development, and secure software. He received his PhD in computer science from K.U. Leuven. *Bart De Decker* is professor at the Computer Science Department of the K.U.Leuven. He received his PhD in computer science from K.U. Leuven. His research interests include secure software, privacy, and anonymity.

Contact: sam.michiels@cs.kuleuven.be / bart.dedecker@cs.kuleuven.be / koen.buyens@cs.kuleuven.be / kristof.verslype@cs.kuleuven.be / wouter.joosen@cs.kuleuven.be

Status: first posted 25/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=167

DRM for digital broadcasting in Japan

By: Kiyohiko Ishikawa, NHK (Japan Broadcasting Corporation), Tokyo, Japan

Abstract: Digital broadcasting has already been operational in Japan for years. All Japanese digital broadcasting is scrambled, but free to air, except for a few Pay TV channels. All contents and copyrights are protected by CAS (Conditional Access Systems). This article describes the current state of these digital broadcasting systems using CAS. It also shows that the realization of content protection and management in broadcasting requires a mechanism to execute some form of enforcement in the STB (Set Top Box).

Keywords: technical analysis – conditional access, digital broadcasting, digital television, DRMS – Japan

Introduction

In Japan digital broadcasting has already been launched. BS (Broadcasting Satellite) started in 2000 and terrestrial digital broadcasting in 2003. All Japanese digital broadcasting is scrambled, but free to air, except for a few Pay TV channels. Content and copyright are protected by CAS. The function of CAS is implemented on a B-CAS card which is an IC card. The function of CAS is described later. Each STB has a particular B-CAS card. The B-CAS card is managed by BS Conditional Access Systems Co., Ltd. (cf. sources). Two types of B-CAS card exist: the red and the blue card. A red card is commonly used for BS, 110 degree CS, and terrestrial broadcasting. 110 degree CS is an independent pay TV service. A blue card is only for terrestrial broadcasting. If no B-CAS card is inserted in a STB, that STB cannot descramble scrambled content. The specification of these digital broadcasting depend on ARIB (Association of Radio Industries and Businesses standards; cf. sources).

The objectives of ARIB are to conduct investigation, research & development and consultation of utilization of radio waves from the view of developing radio industries, and to promote realization and popularization of new radio systems in the field of telecommunications and broadcasting. An important task of ARIB is the establishment of technical standards for radio systems in the field of telecommunications and broadcasting. Overall, ARIB aims at the promotion of public welfare.

The current state of digital broadcasting

10 million STBs were in use for BS digital in September 2005. When terrestrial digital broadcasting started in the Tokyo, Osaka and Nagoya areas on December 1, 2003, the number of terrestrial digital STBs was about 300.000. In the meanwhile more than 5 million terrestrial digital STBs are being used.

There are eight TV broadcasters including data broadcasting, four data broadcasters and five radio broadcasters in BS digital broadcasting. HDTV (high definition) and SDTV (standard definition) services are respectively seven and two channels.

The digital terrestrial TV broadcasts have also the high picture and sound quality of digital high definition (Hi-Vision) and attractive interactive features. Data broadcasting in Japanese characters provides information tailored to each locality. The digital terrestrial broadcasts are received by UHF antenna. The reception of sound and images is clear even on the STBs installed in moving trains, buses etc. A service for simple moving images, data and radio reception on mobile terminals etc. is also anticipated.

There are NHK and five commercial broadcasters which are major network TV companies and two local broadcasters in Tokyo area. Thus Japanese digital broadcasting which uses CAS is successfully spreading.

DRM in digital broadcasting systems

Japanese broadcasters encrypt content for copy protection, regional control of viewing, pay TV charging, etc. The encrypted content is transmitted to the subscriber's STB, which

decrypts the encrypted content. Since each STB has a decryption key in its B-CAS card, it can decrypt content. It is possible to distribute different decryption keys to STBs in different areas, and thereby enable regional control of viewing. For pay TV, only the subscribers who sign a contract with a broadcaster can get a decryption key, and in this way broadcasters control access to the content.

The DRM standardized in Japan employs a three-step encryption system. The subscriber reveals his/her identity to a broadcaster and gets a B-CAS card. The B-CAS card is used as a tamper resistant module. Each B-CAS card has a unique master key, *Km*, that is stored in the tamper-resistant part of the card. *Km* is shared with broadcasters and is used to encrypt personal contract information when the broadcasters transmit information to a subscriber's STB. *Figure 1* shows a block diagram of the conventional DRM system for the Japanese digital broadcasting system.

In the broadcasting station, contents are scrambled with a scramble key, *Ks*. The scramble key is encrypted with a work key, *Kw*, and the work key is encrypted with a master key, *Km*. After that, the encrypted contents and keys are multiplexed and transmitted to the subscribers' STBs. This procedure is called a three-step encryption.

The STB receives the encrypted contents and keys and de-multiplexes the encrypted content, scramble and work keys. It sends the encrypted session and work keys to the B-CAS card, which has been put in the STB. The B-CAS card decrypts the work key with the master key it holds, after which it decrypts the session key with the decrypted work key. The STB then gets the session key from the B-CAS card and decrypts the encrypted contents. In this way, subscribers can watch/listen to the content.

Of these three keys, *Ks* is changed every few seconds when the contents are encrypted to ensure security. *Kw* is the key that authorized subscribers get when they make a contract with a broadcaster. This key is updated with every contract. *Km* is a private key, and it is used to encrypt each contract when the contract information is sent to the B-CAS card. If broadcasters were to transmit *Kw* to all subscribers, they would need to encrypt and broadcast all the *Kw*s. Such a broadcast would require a capacity in proportion to the number of subscribers, and thus it would impose a large load on the transmission channel. To decrease the load, *Kw* is broadcast only when it is to be updated. With these three keys and three-steps encryption, broadcasters can protect the copyrights of their contents. Moreover, to control the viewing region, as *Kw* is encrypted with *Km* and transmitted, broadcasters have to know each subscriber's (B-CAS card's) location.

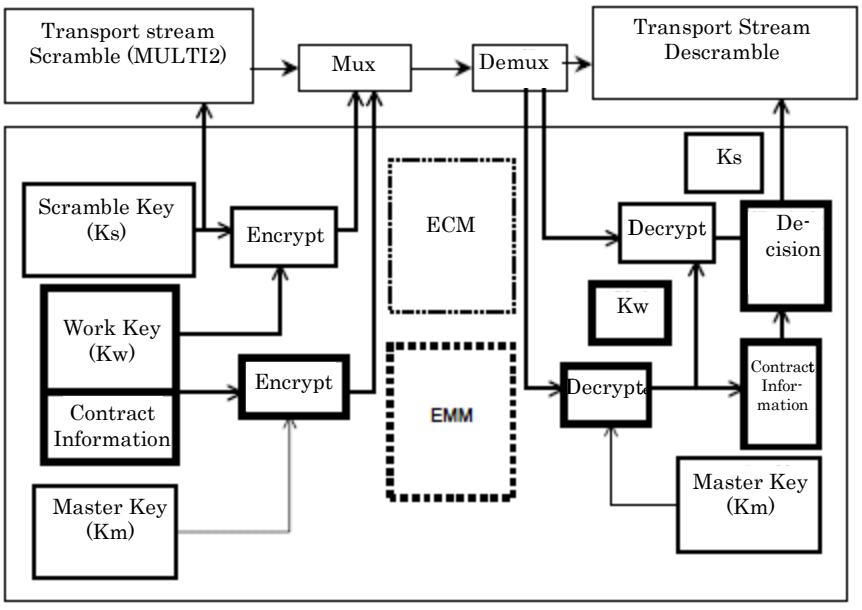


Figure 1: Conventional DRM system

Broadcasters then transmit the encrypted *Kw* to the subscribers that are in the region where the program is allowed to be viewed. This system can control viewing region. For pay TV, *Kw* is transmitted to subscribers who pay for programs or for channels. This system can realize pay TV.

Broadcasting System based on home servers

Broadcasting System based on home servers is a next-generation broadcasting system that utilizes a PDR (personal digital recorder) which is an STB with a large capacity storage, and it is now in the process of being standardized. It employs a four-step encryption. *Figure 2* shows the block diagram of the proposed DRM for Broadcasting Systems based on Home Servers. It is assumed that the transmitted contents will be stored in the receiver, and it is required that conventional broadcasting services can be also received. Hence, the proposed DRM can be constructed by adding a new encryption key to the conventional DRM. The new key is called "content key" (*Kc*), and it is used to encrypt the session key when the content is stored in the PDR. *Kc* may be unique for each content. But actually *Kc* does not have to be unique for each content. It depends on the broadcaster.

Moreover, another new key is introduced. It is called "group key" (*Km'*). But *Km'* will be called domain key with use home network. STBs with the same Km' belong to the same domain. STBs in the same domain are able to use each other's stored contents because they have the same encryption key *Km'*.

Km' is set in the CAS card. As shown in *Figure 2*, *Kc* is encrypted with *Km'* and stored in the STB. *Ks* is also encrypted by *Kc*. Since each STB's *Km'* is different from any other *Km'*s belonging to other CAS cards, once *Kc* is encrypted with a *Km'* of a specific CAS card, it is impossible to decrypt the correct *Ks* by using a *Km'* of another CAS card. Hence, it is impossible to decrypt correctly content from the stored encrypted content that is moved or copied from another subscriber's STB.

Furthermore, Broadcasting System based on Home Servers uses Rights Management and Protection Information (RMPI). RMPI includes copy control information, playback control information, region information, output device control information, etc. When the content is used, the PDR checks the RMPI and controls its processes accordingly.

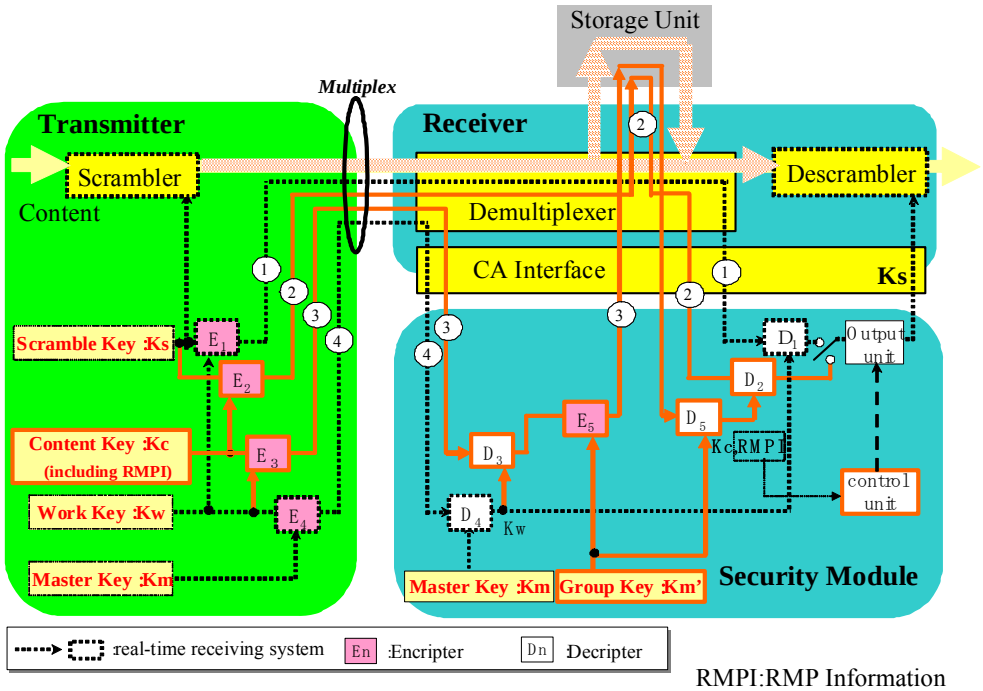


Figure 2: DRM for Broadcasting System based on Home Servers

Content copy control

The realization of content protection and management in broadcasting requires a mechanism to execute some form of enforcement in a STB, which would operate according to content protection related con-

trol data transmitted along with regularly broadcast programmes. Digital broadcasting in Japan transmits encrypted content to achieve such enforcement, based on confidential data provided, including a decryption key. Such confidential information is provided in the form of an IC card (B-CAS card).

With regard to content protection and management, additional consideration should also be given to PDR that can record and reproduce digitally formatted programs without conversion (D-VHS, HDD, etc.). These recording and reproduction systems are designed on the premise of a high-speed digital interface (IEEE1394) connection, protecting digital content under a de facto standard (e.g. DTCP). For this reason, interfaces are also provided for transmitting content protection control data to recording devices and other systems over broadcast.

Regarding re-transmission to the Internet, a flag, or encryption mode, is prepared for a Content Availability Descriptor to enable receiver control.

The relationship between content protection and management requirements and a part of RMPI transmitted via broadcasting is described in the inserted *Table 1*. It prohibits a receiver from having the capability to send the designated contents, which either include a copy restriction by Digital Copy Control Descriptor's "digital recording control data" or has copy protection specified by the Content Availability Descriptor's encryption mode, to any output that could potentially allow the content to be re-transmitted over the Internet. Re-transmission to the Internet is prohibited in those cases where the encryption mode is "0" or copying is restricted by "digital recording control data.

Table 1: Copy control specification

Contents protection requirements		Data transmitted via broadcast				Descriptor			output	
Digital Copy Control	Analog Copy Control	Digital Copy Control Descriptor operation			Content Availability Descriptor operation	Digital Copy Control		Content Availability Descriptor	Analog video	Digital audio
		copy_ control_ type	digital_ recording_ control data	APS_ control _data	encryption_mode	copy_ control_ type	digital_r ecording _control _data	Encryption_mo de		
Copy-freely	Copy-freely	01	00	00	0	01	00	1	CGMS-A: 00 Macrovision: off*	SCMS: Copy-freely
Copy-freely					1					
Copy-never	Copy-never. It can be copied only for conventional analog input recording, since Macrovision is not attached.		11	00	1			0	CGMS-A: 00 Macrovision: off*	SCMS: Copy-freely
	Copy-never.			Non-00	1					
Copy-one-generation	Copy-one-generation. It can be copied only for conventional analog input recording, since Macrovision is not attached.		10	00	1		10	Don't care	CGMS-A: 10 Macrovision: off*	SCMS: Copy-one-generation.
	Becomes Copy-never after one copy.			Non- 00	1		11	Don't care	CGMS-A: 11 Macrovision: APS	SCMS: Copy-never.

Bottom line

Digital broadcasting receivers will be distributed with a key for broadcast viewing, on the condition that they operate according to the signals transmitted via the broadcast. Thus Japanese digital broadcasting is scrambled but free to air. This situation differs from the US and the EU as it is accomplished by CAS technique. CAS is mandated for ARIB (STD-B25) standard receivers. Scrambling contents does not necessarily require mandating a broadcast flag like in the US because the contents are protected by CAS.

Sources

- Asia-Pacific Broadcasting Union (ABU) : http://www.abu.org.my/public/index.cfm
- Association of Radio Industries and Businesses standards: http://www.arib.or.jp/english/index.html; Relevant standards and guidelines developed are:

- ARIB STD-B10 Service Information For Digital Broadcasting System
- ARIB STD-B21 Receiver For Digital Broadcasting (Desirable Specifications)
- ARIB STD-B25 Conditional Access System Specifications for Digital Broadcasting
- ARIB TR-B14 Operational Guidelines for Digital Terrestrial Television Broadcasting
- ARIB TR-B15 Operational Guidelines For Digital Satellite Broadcasting

- BS Conditional Access Systems Co., Ltd.: http://www.b-cas.co.jp
- The Association for Promotion of Digital Broadcasting: http://d-pa.org
- The Association for Promotion of Satellite Broadcasting: http://www.bpa.or.jp

About the author: *Kiyohiko Ishikawa* received the Ph. D. degree in engineering from Nagoya University, Aichi, Japan in 2004. He joined Japan Broadcasting Corporation (NHK), Tokyo, Japan, in 1990, where he is now with the Science and Technical Research Laboratories. Since 1992, he has been engaged in research on magnetic recording head and media and signal processing for high-density magnetic recording systems and on broad-band and high-speed optical disk recording. He currently researches security system for digital broadcast based on home servers.

Status: first posted 25/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=166

The Sony BMG rootkit scandal

Consumers in the US finally wake up. And march to courts…

By: Natali Helberger, IvIR, Amsterdam, The Netherlands

Abstract: The article will have a closer look at the charges of the EFF and a Californian lawyer against Sony BMG's latest DRM strategy. The Sony BMG case adds a number of new dimensions to the DRM and Consumer debate. The article will highlight some aspects, also against the background of similar recent case law in Europe.

Keywords: legal analysis – consumer protection, data protection, DRMS, music industry, DRM users – USA

Introduction

Dark clouds are gathering above the US headquarter of Sony BMG in New York. Complaints are showering down on the enterprise. Class actions zig-zag the once so blue sky of the world's second largest entertainment company. Sony BMG is in deep trouble, and the forecasts are on "storm".

All this because of a small piece of software, Sony BMG's newest Extended Copy Protection technology – XCP, developed by First4Internet (cf. also the INDICARE Monitor article on intrusive DRM by Bohn 2005). Apparently, Sony BMG could not resist the temptation to pack more functionality into its DRM than is really needed to protect contents against unauthorised copying. After all, who would care? Or, to speak in the words of Sony BMG's global digital business division president *Thomas Hesse*: "Most people, I think, don't even know what a rootkit is, so why should they care about it?" (cited in EFF 2005). For those, who still do not know what a rootkit is: a rootkit is a piece of software that cloaks processes, files and logs from a computer's operating system or from its anti-virus programs with the effect that the owner of the computer will not notice that certain routines are performed on his or her computer, or that the software disturbs the transmission of data from terminals, CD drives or keyboards. Sony BMG's XCP installs, unnoticed by the user, a piece of software that prevents consumers not only from copying the content of a CD more often than the allowed three times. XCP recognises and registers the CD that is played on a computer,

identifies the IP number of the computer, is able to monitor and report user behaviour back to the firm, manipulates parts of the computer memory, crashes applications or the entire Windows operating system, interferes with file copying software and other media players and, accidentally, offers shelter for viruses, worms and other nasty things. Attempts to remove the software can lead to system crashes, malfunctions, un-usability of the CD drive and other damage at consumer's computers (Russinovich 2005a).

Luckily, somebody knew what a rootkit is, and could recognise one when he saw one. *Mark Russinovich*, chief software architect at Winternals Software Inc, discovered to his dismay that the Sony BMG CD "Get Right with the Man" by the *Van Zant brothers* installed not only an "underhanded and sloppily written" (Russinovich 2005a, but see also Hamm 2005) piece of software, but also a potentially harmful one. Russinovich documented his discovery on his blog, and the story soon made its way into the media. Comment from Russinovich: "This is the case of the blogosphere having an impact, at least for the moment" (Russinovich 2005b). The impact will be not just for the moment.

Class actions against Sony BMG based on consumer law

The first class action against Sony BMG on behalf of Sony BMG CD buyers was brought by a Californian lawyer, *Alan Himmelfarb*. One of the many things that is special about this case, is that, at least to the knowledge of the author, this was one of the first occasions that in the US an action on the basis of consumer law was brought against DRM. Until now, in the US the DRM discussion was generally kept in the copyright domain (see e.g. Liu 2003, Cohen 2005). Himmelfarb accused Sony BMG of the violation of Sections 1770 (a) 5 and 9 of the Californian Civil Code (this title in the Californian Civil Code is also known as the Consumer Legal Remedies Act; cf. sources). Section 1770 (a) 5 and 9 ban representing that goods or services have characteristics which they do not have, comparable to the European provision on misleading practices. According to Himmelfarb, by concealing the existence of the rootkit program, and what it does once installed on a user's computer, Sony BMG has violated both sections of the Californian Civil Code and has committed unfair, deceptive and misleading business practices.

Not content with that, the Electronic Frontier Foundation (EFF) brought a second class action complaint against Sony BMG's XCP technology. The EFF charge also includes the MediaMax technology used by Sony BMG. The EFF found that the MediaMax DRM has characteristics very similar to those of XCP. Again, the EFF claim is based on the Consumer Legal Remedies Act.

Scrutiny of the Sony BMG's EULA

In addition to the charge about misleading practices, the EEF complained about Sony BMG's provisions in the consumer contract, in form of Sony BMG's End User Licence Agreements ("EULA") for the XCP and MediaMax CDs. The EEF had a closer look at the EULAs and found, indeed, rather bizarre conditions:

- restrictions on the user's ability to use the digital content on the CD in the event that that consumer chose to leave the United States, *speak*: once you leave the country you are no longer allowed to listen to any of the CDs you purchased.
- restrictions on resale and transfer of the digital content on the CDs, *speak*: no way that you can get rid of your infected CD by selling it to your uncle or at the flee market.
- restrictions on the user's ability to use the digital content on the CDs at work, *speak*: you go to work, the music stays home;
- restrictions on the user's ability to use and retain lawfully made copies of the digital content on the CDs in the event that the original CD is stolen or lost, *speak*: should anybody nick your CDs, you are obliged to also delete all remaining copies that you might have made, as if you didn't have enough trouble already;
- restrictions on the user's ability to use the digital content on the CDs following

a bankruptcy, *speak*: if you've lost your money you're are not worthy to listen to Sony BMG music;

- conditioning the user's continued use of the digital content on the CDs on acceptance of all Sony BMG software updates, *speak*: you have to accept all updates that Sony BMG wants to smuggle onto your computer, or: forget about listening to your CD;
- restrictions on the user's ability to examine and test his or her computer to understand and attempt to prevent the damage caused by the rootkit, *speak*: maybe you have a bad feeling with that CD, maybe you are a second Russinovich, still, Russinovitch-like self-help actions are not part of your contract, sorry;
- a reservation of rights by Sony BMG to use "technological 'self-help' measures" against the computers of users who desire to make use of the digital content on the CDs "at any time, without notice to [the user]"; *speak*: Sony BMG reserves the right to happily install more anti-copying protection ever after, and you are not even entitled to know about it;
- and… and… and. (EFF 2005).

Without accepting the EULAs, consumers will have no access to the CD. This is hard, considering that they have already purchased the CD. It remains to be seen how the judge will decide. In the US, contractual freedom is a highstanding value, which makes it at least doubtful if the judge will find these restrictions unconscionable.

The two cases (and more are on the way; e.g. the Attorney General of Texas brings a suit against Sony BMG in Texas; cf. The State of Texas 2005) confirm once more that DRM is not only a matter of copyright law, but that it touches, much more broadly, on valid interests of consumers, those who purchase digital content for own, private use. EEF's allegations concerning MediaMax, moreover, show that the rootkit scandal was not simply an accident, but part of an established business strategy of one of the largest music publishers in the world. The cases are in line with earlier cases in Europe where consumers claimed that the CDs they bought were defective products, due to the restrictions imposed by the DRM (Helberger 2004, 2005 a, b). The Sony BMG case, however, adds a number of new dimensions to the existing experiences with claims against DRM. This is why it is interesting to look at some details of the claim more closely.

Unfair competition law

Interestingly, Californian law knows another provision. In Division 8 of the Business and Professions Code (cf. sources), i.e. California's unfair competition law, which was also evoked by both, Himmelfarb and the EFF against Sony BMG, Section 22947 contains what is called the Consumer Protection Against Computer Spyware Act (cf. sources). Unfair competition law plays an important role in terms of consumer protection in California, as it includes a number of consumer friendly provisions. The Consumer Protection Against Computer Spyware Act prohibits a person or entity other than the owner of a computer to insert without authorisation spyware on that person's computer, that is software that:

- takes control of the computer;
- modifies internet settings;
- collects personal information;
- prevents efforts to block the installation of that software;
- pretends that the consumer can de-install the software, if in reality she cannot do so;
- removes, disables or renders inoperative security, anti-spyware or antivirus software installed on this computer.

In other words, the law, which passed Senate in August 2004, seems to have been written with an eerie foresight of the Sony BMG case. European consumer law does not know any comparable rules. The closest to this are probably national provisions on computer tampering in national penal codes.

It remains to be seen how the Superior Court of the State of California will decide – if it will decide at all. Presently, there are strong indications that Sony BMG will do its best to avoid a decision and settle the cases brought

against it. EFF requests that Sony BMG will be obliged to:

- widely and detailed publicise the potential security and other risks for consumers associated with XCP and MediaMax technology;
- cooperate fully with manufacturers of anti-virus or similar security tools to facilitate the complete removal of XCP and MediaMax from infected computers (something which is, so far, not possible);
- refund the purchase price of the CDs containing MediaMax or XCP and
- to refrain from further abuses.

The last claim is interesting insofar as it is not restricted to appropriate labelling, as was claimed in the EU cases. Instead, the plaintiff demands that Sony BMG will avoid further abuses, making evident that Sony BMG's invasive technology should not be accepted under any terms, even if consumers receive a prior warning.

Another interesting characteristic of the US cases is their nature as class action – an accepted procedural instrument under US consumer protection law. EFF pointed out, very correctly, that it would be impracticable and prohibitively expensive if all members of the class sued individually. The damages suffered by each consumer were relatively small, too small to justify the high expenses for individual prosecution in a matter that is as complex as the present case. As a result, consumers would probably not sue on an individual basis. Moreover, as EFF also pointed out, a multitude of individual claims poses a serious strain on the functioning of the court system. These are problems that are equally critical in Europe and render the instrument of consumer protection law in DRM cases less effective; the situation in Europe is complicated by the fact that most European member states do not acknowledge the instrument of class action.

Finally, to mention a third interesting detail and difference to the European cases: neither Himmelfarb nor the EFF sought to use consumer protection law as a means to protest against the restriction of usage possibilities through DRM (e.g. private copying) or to make an argument in favour of fair use. In contrast, DRM and the private copying exception were at the heart of most of the existing claims in Europe. To the knowledge of the author, no (successful) attempts have been made in the US so far to use such a thing as warranties law as a means to enforce the private copying exception (as was done in Europe). The author was rather puzzled about this finding and tried, subsequently, to identify if this difference is the result of US consumer protection law and policy, or if it is by accident that yet no action in this respect has been taken in the US.

The answer must remain somewhat speculative. Partly, the reason might have to do with the structure of US copyright, notably the fair use defence. Unlike in Europe, in the US there is little discussion about if copyright law conveys a right to private copying. It is widely acknowledged that fair use is an affirmative defence, not a right. However, because the fair use principle is far broader than the European private copying exception, and because fair use cases are able to accommodate different interests beyond the making of private copies, the fair use doctrine invites far more readily attempts to adapt copyright law in a way to accommodate user interests (Cohen 2005, Liu 2003), without seeking recourse to consumer protection law. This may explain, why in the US, the DRM discussion has concentrated so far mostly on the copyright domain.

On the other hand, its vagueness and the lack of a clearly encircled (that is: worded) protection worthy consumer interest (e.g. private copying) in US copyright law may be a reason, why consumer protection law is of little use to enforce an existing standard in copyright law. Such a standard simply does not exist, at least not in form of clearly carved out copyright exceptions. This observation leads to the other part of a possible answer, why US consumer protection law was not used so far to enforce user interests in e.g. private copying. The respect for contractual freedom and the contractual autonomy of private parties is particularly strongly developed in the US. In general, the idea is that the state should refrain from interfering with the

actions of private parties as much as possible. In contrast, in Europe the concept of the positive protection duty of the state, i.e. the state's duty to actively create an environment that is favourable to consumers' interests, is far more commonly acknowledged. Finally, in both, the US and Europe, a general idea prevails that consumer protection law protects in the first place individual consumer interests, and is less suitable to protect public policy interests, such as broad availability of services, stimulating creativity and innovation, etc.

Bottom line

The cases brought by Himmelfarb and the EFF are in many respects a primer. They also introduce us to the US consumer protection law as a possible remedy against DRM misuse, next to copyright law. We can await with suspense the decision by the Superior Court of the State of California, and whether it will trigger a wider reaching discussion about consumer protection in the IP sector in the US. One can hope so, because US law knows a number of interesting tools to improve the legal standing of consumers, be it the institute of class action, be it special rules about spyware. One the other hand, chances are high that this case of consumers suing an undertaking because of unfair practices will be, as so many others before it, settled before the judge will have a chance to make a final statement. Even so – some hairy questions are on the table! And, hopefully, they cannot be removed from there by simply giving each affected consumer a new CD or a voucher for some free downloads. This is about more than just a new CD.

Sources

- Bohn, P. (2005): Intrusive DRM: The cases of Sony BMG, StarForce and Microsoft. INDICARE Monitor, Vol. 2, no 9, November 2005; http://www.indicare.org/tiki-read_article.php?articleId=155
- Cohen, J. (2005): The place of the user in Copyright Law, 74 Fordham Law Review (forthcoming)
- Consumers Legal Remedies Act: http://www.harp.org/clra.htm
- Consumer Protection Against Computer Spyware Act: http://pub.bna.com/eclr/sb1436.htm
- Division 8 of the Business and Professions Code: http://caselaw.lp.findlaw.com/cacodes/bpc/17200-17210.html
- EFF (2005): Class Action Complaint before the Superior Court of the State of California, County Los Angeles, available at: http://www.oag.state.tx.us/newspubs/releases/2005/112105sony_pop.pdf
- Hamm, S. (2005): Sony BMG's costly silence, Business Week Online, November 29, 2005, available at: http://www.businessweek.com/print/technology/content/nov2005/tc20051129_938966.htm
- Helberger, N. (2004): It's not a right silly! The private copying exception in practice. INDICARE Monitor, Vol. 1, no. 5, October 2004; http://www.indicare.org/tiki-read_article.php?articleId=48
- Helberger, N. (2005a): Thou shalt not mislead thy customer! The pitfalls of labelling and transparency,. INDICARE Monitor, Vol. 1, no 9, February 2005, http://www.indicare.org/tiki-read_article.php?articleId=76
- Helberger, N. (2005b): Not so silly after all. New hope for the private copying exception, INDICARE Monitor, Vol. 2, no 6, August 2005; http://www.indicare.org/tiki-read_article.php?articleId=132
- Liu, J. (2003): Copyright Law's theory of the consumer. Boston College Law Review, Vol. 44, 2003
- Russinovich, M. (2005a): Sony, Rootkits and Digital Rights Management gone too far. Blog, available at http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html
- Russinovich, M. (2005b): More on Sony: Dangerous decloaking patch, EULAs and phoning home; Blog, available at http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html
- The State of Texas v. SONY BMG Music entertainment, LLC (2005); http://www.oag.state.tx.us/newspubs/releases/2005/122105sony_lawsuit.pdf

About the author: Dr. *Natali Helberger* is senior project researcher at the Institute for Information Law, University of Amsterdam, and managing legal partner in the INDICARE project. Dr. Helberger specialises in information law, technical control of information, the interface between law and technology, and between media, intellectual property and telecommunications law. Presently, she is staying as visiting scholar at the University of California, Berkeley. Contact: helberger@ivir.nl

Status: first posted 09/01/06; licensed under Creative Commons
URL: http://www.indicare.org/tiki-read_article.php?articleId=165

Editorial of INDICARE Monitor Vol. 2, No 12, 24 February 2006

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The current issue contains 15 articles: the first and the second are appetizers for new INDICARE documents (second survey and fifth workshop). Four excellent articles deal with contracts, copyright confusion, court decisions, and the copyright reform in France. We also report about the DRM session of a recent OECD conference on the digital economy, and review an empirical study which tested the privacy conformance and user-friendliness of DRM systems. The focus theme "Trust, DRM, and TC" is approached in six different ways – among them the ambitious approach of OpenTC, a large project funded by the European Commission.

Keywords: editorial – INDICARE

Two new INDICARE documents published

INDICARE proudly presents the findings of its second European consumer survey. While the first focussed on music consumption, this one is about European Internet users consuming *digital video content*. The article by *Nicole Dufft* of INDICARE Partner Berlecon Research – responsible for the survey – summarizes the main findings. It shows that digital video content is becoming popular in Europe. We learn about consumers' usage habits and expectations, about their willingness to pay for usage rights and their awareness of DRM. The complete survey results are available for free (Dufft et al. 2006).

Kristòf Kerényi, SEARCH Laboratory, organizer of the fifth INDICARE workshop on "Human Factors of DRM" summarizes what he personally found the most interesting facts and conclusions. He especially highlights the session about accessibility for the blind, and the presentations from consumer initiatives. The official report of the workshop, which took place in Budapest on 19 January 2006, will be available from the INDICARE Website in March 2006.

More about the present issue

Contracts, copyright, and courts

Lars Grøndal, a legal advisor for the Consumer Council of Norway, currently working for BEUC (The European Consumers' Organisation), digs into the contractual terms consumers often accept without being aware of the content. The focus is on contract terms with respect to DRM in the field of online music. The "Terms of Service" (ToS) of iTunes are taken as an example. The article reveals that these ToS contain unfair terms not conforming with the law. In Norway, the Consumer Council has therefore complained to the Consumer Ombudsman in order to get iTunes terms amended. However, as Grøndal makes clear from the beginning, his article is not primarily about iTunes. The type of unfair terms identified is not unique to iTunes, indicating a more general problem in online markets for digital goods and thus constituting a public policy issue.

Matthias Spielkamp, iRights.info, starts from the assumption that the implementation of the EUCD confuses consumers and has made copyright an enigma for laypersons. This point is demonstrated impressively by a case study looking at file-sharing in the light of corresponding legislation in Germany. His conclusion is that publicly funded, impartial consumer information is needed as rights holders can not be expected to provide it. iRights.info, funded by the Ministry for Consumer Protection in Germany, is of course an initiative he has in mind. Beyond the national level he sees a need for multi-national, multi-language efforts at the EU level.

Natali Helberger, IViR, INDICARE's most eloquent legal expert has already been watching developments in France for a while. This time she contributes two closely related pieces of legal analysis.

The first article discusses the latest court decision in France with respect to private copying of protected content: *Christophe R. vs Warner Music*. The court concluded that TPM has to respect the private copying exception. This case underlines that until now,

courts had to deal with consumers' complaints about copy-protected CDs or DVDs, while the legislator hesitated to implement the EUCD

And that's exactly the subject of Helberger's second article *Vive la Balance! Pleading for a French revolution of copyright*. The French Parliament launched "Le Project de Loi N° 1206" in order to bring about the long-pending implementation of the EUCD, including, of course, the provisions about TPM.

The analysis of the draft shows Natali's disappointment. Given the vivid public debate about DRM and consumers, and the recent court decisions, the drafted law falls short of expectations. To hold DRM *users* liable for compliance with the law is regarded as a step in the right direction. She criticises, however, that such obligation is of little value without accompanying measures that guarantee its enforcement

By the way, despite the title, Natali is not really pleading for a new revolution. "Creating the conditions for a more consumer-friendly DRM environment is not revolutionary…" she says. But sometimes a necessary reform in a difficult environment against the mainstream might be worth being called a revolution anyway.

Alternative models for content distribution

Daniel A. Nagy, developer of the ePointSystem, working with INDICARE partner SEARCH, comes up with an interesting content distribution framework. The proposed framework relies on peer-to-peer digital payment. It aims at unprotected content, however DRM techniques can aid the business models to become more efficient by reducing transaction costs, e.g. reducing the load on the operators or helping to exclude free-riders. In these scenarios, users of DRM-enabled devices, i.e. consumers, have no incentive to attack DRM systems.

OECD conference report

Philipp Bohn, Berlecon Research, reports about the Future Digital Economy conference, Rome, 30 and 31 January 2006, which was organized by the OECD and the Italian Minister of Innovation and Technology. More precisely he summarizes what was said about DRM at the conference, and in particular during a panel session addressing "Content diffusion: IPR, DRM, licensing, content security, standards".

Review of privacy4DRM

Knud Böhle, ITAS, reviews a study sponsored by the German Ministry for Education and Research (BMBF). *Privay4DRM* appears to be a noteworthy contribution to conformance testing of DRM systems with respect to privacy and data protection provisions. The scrutiny of data flows and data traces when using DRM systems reveals significant shortcomings. The authors propose to improve the situation by more transparency, end-user involvement, pseudonymity options, and "privacy labels".

Focus theme: Trust, DRM and TC

Mark Bide, Senior Consultant, Rightscom Limited, holds that "informed consumers should welcome the implementation of effective DRM – if it meets their needs". This article can be read as a kind of introduction to the focus theme as it opens up the broader perspective. The general message is that we must think in terms of "network citizenship", which includes as a major task managing trust on the network. The core concept he introduces is "Digital Policy Management", a concept which allows for combinations of trust, good will, law and technical protection measures. "Consumers", he says, "will welcome the introduction of digital policy management technology … only if it also offers a solution to *their* underlying security and identity problems and contributes to the maintenance of civil society on the network, with all the complex checks and balances that this implies."

Robert A. Gehring, member of the research group for Computers & Society at the Technical University of Berlin, explains – as precisely as possible within a short article – the relationship between trusted computing (TC) systems and digital rights management (DRM). In his view TC components are tools – in themselves neither good nor bad – which can be used to build DRM systems or to protect "darknets". He warns that strong DRM systems based on TC do not *per se* guarantee

successful business models if consumer expectations are not met.

The next article by *Dirk Kuhlmann*, Hewlett Packard Laboratories, Bristol, describes a new Integrated Project (IP) funded by the European Commission, called OpenTC. Kuhlmann has the overall technical lead for the OpenTC project. OpenTC aims to combine TC technology and FOSS and to demonstrate advantages of this approach. The author is convinced that enhanced protection and security based on TCG technology will become standard, and that professional users of non-proprietary operating systems (like Linux) and software will ask for comparable protection mechanisms – independent of whether FOSS communities like it or not. OpenTC aims to fill this gap. Furthermore it claims that the combination of TC and FOSS will have advantages in terms of privacy, efficiency, openness, and consequently user acceptance. The author is fully aware that a lively public discussion is going on about TC, and about the possible combination of TC and FOSS.

Florian Schreiner, *Michael Pramateftakis* and *Oliver Welter*, computer scientists from Munich University of Technology, are partners in the OpenTC project aiming to create a DRM system which governs the use of all kinds of sensitive data from the medical sector to entertainment. The system proposed differs from others, because it will be open-source and will use the TPM-Chip to enforce security. Advantages expected are: interoperability with other DRM Systems, transparency, convenience for users, and support of legacy software

Gergely Tóth, SEARCH Laboratory, writes about the next version of the Symbian operating system for mobile phones, which incorporates Trusted Computing based security features. Mobile phones using the Symbian v9.1 operating system will probably be used for DRM-based applications. Multi-media phones like Nokia N91 and the Sony Ericsson W950i said to implement the Symbian operating system and provided with a 4 GB internal hard disk obviously point in that direction of mobile phones able play and to handle protected digital music.

Last not least *Arnd Weber*, ITAS, Karlsruhe, and his brother *Dirk A. Weber*, an IT-Consultant, have reviewed recent works by legal scholar *Stefan Bechtold* dealing with the risks of trusted computing from a regulatory point of view. The reviewers present Bechtold's arguments and his general view that there are possibly many risks involved, but that they could be handled by skilful design of TC-architectures and proper institutional arrangements. The main threats identified are: dominance of players, lack of capabilities to deal with copyright exceptions, and loss of privacy.

The reviewers however not only summarize the risks and remedies mentioned by Bechtold, but also critically remark that Bechtold might be overoptimistic as he seems to assume that all the hard- and software built on TCG-principles will work properly. This, however, may not be the case.

Sources

- Dufft, Nicole, et al. (2006): Digital Video Usage and DRM – Results from a European Consumer Survey, Berlin, February 2006; online available at: http://www.indicare.org/tiki-download_file.php?fileId=170

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 06/03/06; licensed under Creative Commons; included in the INDICARE Monitor, Vol. 2, Number 12, February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=187

Digital video usage and DRM

Results from the second INDICARE survey

By: Nicole Dufft, Berlecon Research, Berlin, Germany

Abstract: Commercial services for online digital video content are not yet very common in Europe. But new offerings continue to be introduced to the market, and many of them apply DRM systems. In addition, a large share of unlicensed digital video content is available. It will be crucial for successful commercial services that consumers' demands and expectations about what they can do with the content they obtain are met. The latest INDICARE survey provides information about the usage habits of consumers of digital video, their expectations and their willingness to pay for usage rights as well as their awareness of DRM and related issues.

Keywords: survey – INDICARE, broadband, consumer behaviour, consumer expectations, digital media – Europe, France, Germany, Spain, Sweden, United Kingdom

Objective of the survey

The goal of the two INDICARE consumer surveys was to gather reliable data on the preferences and behaviour of European consumers with respect to digital goods and on their awareness and acceptance of DRM. The first INDICARE survey was published in May 2005 (Dufft, et. al. 2005) and covered digital music usage and DRM. The current survey's focus is on digital video content: the extent to which European Internet users already use video content from the Internet, the channels through which they obtain it, their willingness to pay for certain usage rights, as well as their knowledge and attitude towards DRM. Included in the survey is the usage of digital video files from various sources. Explicitly excluded are watching videos from physical media such as DVDs or Video CDs on the computer and video games.

The survey was conducted among 2,731 Internet users in five European countries: Spain, Germany, France, the United Kingdom (UK) and Sweden. These countries account for about 64% of GDP and 55% of the total population in the 25 member states of the European Union (Eurostat 2006). Results are representative for all Internet users from age 15 in the respective countries with regard to age, gender, as well as Internet usage frequency.

Digital video usage is not yet very widespread in Europe

Results from the second INDICARE survey show that usage of digital video content is still at a relatively early stage in Europe: even though many Internet users (61%) have made first experiences with watching digital video content from the Internet on their computer, only less than a quarter (22%) do so *frequently*. This compares to 34% of European Internet users that frequently listened to digital music on their computers in 2005.

Downloading video content from the Internet is even less common: 38% have tried to download content, but only 14% do so frequently. However, a quarter of all Internet users show interest in downloading video content from the Internet in the future. This indicates that there is potential for future video download services.

Portable video content does not play an important role to date. However, two results might point towards commercial potential for mobile offerings: first, a comparatively high share of mobile video users *frequently* consumes video content on the go (once tried, they stick with it). Second, almost a quarter of all Internet users – younger users as well as older ones – are interested in using mobile video content in the future.

A lack of knowledge and awareness is the most important reason for not consuming digital video content. A shortage of sufficient bandwidth and high costs are currently not

perceived as important barriers, except in Germany.

Significant differences between countries exist

Analysing digital video usage at the country level shows significant differences between the five European countries covered in this survey (Spain, Germany, France, the UK, and Sweden). Spain has the highest proportion of frequent digital video users (46% of all Internet users), followed by France, Sweden, and the UK. Germany has by far the lowest proportion of Internet users frequently consuming digital videos (12%).

These differences can partly be attributed to differences in the Internet population in each country: while Spain has, for example, a relatively low overall share of Internet users in percent of total population, the majority of these users are heavy (i.e. daily) users. Germany, in contrast, has a large Internet population overall, but among these more than half use the Internet only on a weekly basis or less frequently.

Types of video content and channels to obtain it are very diverse

Survey results reveal that the consumption of digital video content is characterized by a high degree of diversity. This diversity relates to the types of video content consumed as well as to the channels accessed to obtain it.

First, we can see that users are trying out many different types of video content and that there is not *the* single "killer content". Music videos are presently the most popular content category, but they are very closely followed by private content (e.g. family and holiday videos), as well as movie previews and advertisements. TV shows and amateur content are currently the least popular content categories. The relatively low importance of amateur content such as video blogs or podcasts contrasts the high attention that this type of content is attracting in the media at present.

Second, there is no single most important channel where users obtain digital video files. Instead, the sources are rather diverse with company websites being the most important source, followed by ripping DVDs and using P2P networks. Service offerings by download portals, mobile operators or TV stations do not yet have a large market penetration.

Diversity needs to be reflected in differentiated usage rights and DRM systems

This diversity in digital video consumption is further aggravated when we look at the different usage rights that consumers are willing to pay for when offered commercial services. A considerable share of users is, for example, willing to pay extra for the right to burn or time-shift full-length movies, while the same is true for a much lower share of users in the case of music videos or TV shows.

The diversity of different content types, distribution channels and expectation of usage rights results in a complexity for content providers and (DRM) technology providers alike, because the diversity needs to be reflected in differentiated service offerings for different content types and channels – particularly with respect to the usage rights granted and the technological measures applied to enforce usage restrictions. As a result, the complexity will affect the way DRM protection is designed, applied and accepted, as the number of technological challenges (e.g. interoperability) is likely to increase.

There is indeed potential for commercial digital video services

Our findings also indicate that there is future potential for commercial digital video content offerings, given that consumers' expectations of what they can do with the content are met. First, a considerable share of consumers indicate that they are interested in watching digital movies and TV shows in the future. Second, many digital video users are interested in services from TV stations, download portals or mobile operators. And third, a significant share of consumers is actually willing to pay for extended usage rights such as burning, time-shifting or sharing.

Digital channels do not necessarily cannibalize existing channels. A considerable share

of users are actually watching or downloading digital versions of a specific video via the Internet that they had already consumed through other channels, for example TV. This indicates that digital video offerings could be well suited as a complement and as a means to exploit the commercial value of movies and TV shows in different stages of their life cycle.

Consumers apparently prefer active over passive content consumption

There are two major advantages that consumers associate with digital video usage: first, being able to watch content wherever and whenever they want (time-shift), and second, being able to avoid commercials. Users are obviously annoyed by the way commercials are placed in traditional media channels today.

At the same time, the high popularity of movie previews and advertisements offered on company websites shows that consumers actively choose to watch smart and entertaining advertisements. This emphasizes, on the one hand, that the Internet can be a very efficient channel for marketers (particularly for the movie industry) to place commercials. On the other hand, consumers increasingly seem to prefer pull (as opposed to push) advertisement.

Consumers' attitude towards content consumption is apparently about to change from passive to more active consumption behaviour, where viewers are in control of their own schedules and content preferences.

P2P networks play a less prominent role for digital video than for digital music

P2P networks play a less prominent role as a source for digital video than is the case for digital music. 27% of the digital music users, but "only" 14% of the digital video users frequently use P2P networks. However, P2P usage has reached a very significant share in certain countries (e.g. 67% of digital video users in Spain compared to only 11% in Germany).

But we also find that P2P still needs time to be accepted by active P2P users as a legal distribution channel. Even though half of all digital video users appreciate the importance of copyright (i.e. they care if a file is copyrighted or not), only a minority of P2P users would continue to use their network after it was transformed into a licensed offering. Given a significant proportion of users that would be willing to pay extra for extended usage rights, we conclude that the absence of usage restrictions is one of the most important factors besides costs that make P2P networks so popular today.

Consumers are not aware of DRM and usage restrictions

Despite the wide application of DRM technologies that restrict usage rights of digital content today, a large majority of consumers has never heard of DRM and does not know that these technologies are applied. This finding confirms results from the first INDICARE survey among digital music users. In addition, the majority of users that have downloaded digital video content were not informed whether usage rights of the respective videos were restricted or not.

Of those users that know about DRM, almost half were not aware of privacy issues related to DRM, e.g. the fact that DRM technology has the potential to monitor uses of digital content and profile consumption behaviour. One third knows about potential privacy issues but does not mind or simply accepts it.

Bottom line

The results show that digital video content is gaining popularity in Europe. However, many users do not use digital videos on a frequent basis. This has a number of reasons, the most important being a lack of information about offerings and prices. We found that there is no single "killer content" in sight, as was the case, for example, with ringtones for mobile phones. The diversity of the digital video ecosystem (i.e. players, types of content, usage rights, distribution channels) is very likely to add complexity to the respective DRM systems, especially concerning interoperability. Although DRM was more broadly discussed in the recent past, we did not find a rise of awareness for DRM on the side of the consumers.

Sources

- Dufft, Nicole, et al. (2005): Digital Music Usage and DRM – Results from an European Consumer Survey, Berlin, May 2005; online available at: http://www.indicare.org
- Dufft, Nicole, et. al. (2006): Digital Video Usage and DRM – Results from a European Consumer Survey, Berlin, February 2006; online available at: http://www.indicare.org
- Eurostat (2006), http://epp.eurostat.cec.eu.int

About the author: *Nicole Dufft* is a senior analyst at Berlecon Research. She has been analysing a variety of ICT topics ranging from mobile computing and application service providing to DRM. Currently, she works in the field "digital consumer". She is a member of the INDICARE project team. Contact: nd@berlecon.de

Status: first posted 23/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=178

Human factors of DRM – A tour d'horizon

Report about the fifth INDICARE workshop

By: Kristof Kerenyi, SEARCH laboratory, Budapest, Hungary

Abstract: The fifth INDICARE workshop on the "Human Factors of DRM" took place in Budapest on 19 January 2006. The workshop informed about technological, legal and consumer protection aspects of DRM including results from several consumer surveys. Two highlights of the event were the session about content accessibility for the blind, and the presentations from consumer initiatives.

Keywords: conference report – INDICARE, accessibility, consumer expectations, consumer interests, disabled persons, interoperability, survey

Introduction

The workshop attended by about 40 persons took place in the Informatics building of our university in Budapest on 19 January 2006. It was organised around five thematic blocks: "consumer surveys", "accessibility", "content providers' experience", "consumer rights" and "consumer initiatives". This report does not aim to sum up everything that was said at the event, it is just meant as an appetizer for the full workshop report which will be available for download on the INDICARE web site in March 2006. Below I try to give a very brief coverage of the interesting facts and conclusions for myself.

Consumer surveys

It is very important to explore usage patterns, and other behavioural aspects of users with regard to digital content, since many experts agree that only such business models can win against traditional non-digital distribution channels and illegal offerings which provide more to the consumer, a value added over the common "buy in the store and own a copy" scenario. The common topic of the first block of presentations was what consumers want, how they use content today, in the early age of digital media, and what they know about DRM.

Alapan Arnab, a PhD student from the University of Cape Town started with a strong statement: DRM used to be a jargon for evil technology, also lately when flops like the recent Sony BMG rootkit case did not do any good for the reputation of digital rights management. He analysed some offerings by international companies, and came to the conclusion that terms of purchase were not well advertised, and this increased consumer distrust. He talked about an on-line survey made by his team, which collected 292 full responses to an impressive 91 questions, investigating consumer habits and attitudes

towards DRM. Respondents were from countries all over the world. Unfortunately he had to rush through his findings to have time for the introduction of "good DRM". This, Arnab said, exploits the opportunities in technology for the benefit of the consumer rather than for mega companies, which use DRM only as an enforcement of copyright. DRM could also be used to protect personal data and ensure privacy, which, for example in the case of protecting medical information, would increase consumer trust in technology.

Dr. *Péter Benjamin Tóth* from ARTISJUS, the Hungarian Bureau for the Protection of Authors' Rights, introduced the results of two surveys to support his statement that Digital Rights Management may not be the best solution to address today's problems, instead Collective Rights Management – which term he preferred instead of calling ARTISJUS a collecting society – could be a better choice. He argued by drawing up the formulas based on which levies are collected, and supported his point with the figures derived from the two surveys. Examining content copied to blank CDs and DVDs, both in a representative survey done by GfK (Gesellschaft für Konsumforschung), and in another done by Free Association at the Sziget festival (the biggest music festival in Central-Europe, therefore the respondents here were "power users" of music) he concluded that at least 90 percent of data burned to blank media was content protected by copyright, but subject to free copying. From this he derived the calculated amount of levy per carrier that *should be* a fair compensation for authors, and then showed the *actual amount from use*. Interestingly, even though the amount from use was at least 5 times smaller than the smallest calculated amount, most consumers think even this small amount unfair for themselves. Levies have to be held so low, Tóth said, because there is a strong black market presence also on the market of blank CDs and DVDs, with which they have to compete, and consumers, here too, vote with their wallets.

Philipp Bohn, analyst and INDICARE team member from Berlecon Research, talked about the results of the first consumer survey on digital music (Dufft et. al. 2005) and introduced the second consumer survey on digital video use, which was at that time being prepared, although it is now online on the INDICARE web site (Dufft et al. 2006).

Accessibility

Norbert Márkus from the KFKI Laboratory of Speech Technology for Rehabilitation, and also a jazz pianist and composer gave a very extensive introduction to the history of accessibility on the computer. He said that in the 80s and early 90s blind people were in a not much worse situation than their sighted colleagues. Then with the coming of window-based systems (also Microsoft Windows) their situation got much worse, but by today the technology has improved to work again with the latest computers. However, nowadays the problems are due to carelessly designed layout. DRM means another difficulty for accessibility, since, though allowed by copyright law, making content accessible for the blind would mean in many cases making it available for content pirates, too. At least the content publishers have this opinion, which, again, means great difficulty for blind or partially sighted people. Márkus talked also about musical scores in Braille form, which are represented in computers as BMX (Braille Music XML). The situation with this is the same as with other content: publishers fear of pirates.

Hugh Huddy from the Royal National Institute of the Blind, head of Campaign for good E-Document Design, gave a talk about new opportunities and hurdles that e-documents pose for the blind. After demonstrating some special programs that make laptops, mobile phones and other electronic staff blind-friendly, Huddy talked about a new world where paper is gone. This opens up the opportunity for blind and partially sighted people to have an equal chance in life for accessing information, but he said, just as we create artificial barriers for handicapped people in the physical world, we are re-creating such barriers for the blind in the electronic world. He emphasised the responsibility of technology companies, policy makers and also users to create a world where the "Right to Read" is reality.

Content providers' experience

The rather short session where two large telecommunication providers, T-Online and T-Mobile, introduced their view of DRM inspired a lively debate.

Miklós Gyertyánfy from T-Online talked about the T-Group member's music offerings and use of DRM (also covered in Kerenyi 2005), and also introduced their video-on-demand service. They chose Microsoft's solution because it is compatible with most players. He also underlined that while they have the intention, it is not yet possible to introduce electronic video sell-through (download and burn), since MS technology does not support it. Gyertyánfy talked about T-Online's new pilot project with IPTV, into which they will incorporate all previous DRM-related experience. The most important, he said, was: users don't want to understand technology, just use the content anytime, anywhere.

Péter Verhás from T-Mobile talked about the technical solutions which are used to protect content. He talked about OMA DRM 1, which is used by the vast majority of phones today, using the phone as authentication token, not the SIM card, which means that interoperability was not even an issue when the system was designed. However, as in the case of T-Online, they provide a "reload" service for the new device: the content provider has a record of what the consumer has purchased, and enables her to re-download the content for the new device. Registering what a consumer has purchased also gives the advantage for the content providers of knowing the customer, and his habits. This and the contractual relationship between the telecommunications provider and the consumer puts mobile operators at an advantage. Verhás had another very important point in his presentation: he emphasised that while mobile phones are becoming the DRM enabler devices today, their usage pattern differs between countries, thus cell phones do not enable content usage and DRM in the same way across cultures.

Both speakers attracted a huge wave of complaints and questions regarding their services and attitudes towards consumers: it seemed like as they were the only representatives of the content providers, some workshop participants blamed them for the current, in many cases unfriendly situation with real world content offerings.

Consumer rights

One of the questions most interesting to consumers is their rights, and legal state when dealing with digital content. Consumers are often criminalized, advertisements on the streets and television spots emphasise that downloading music is illegal. On the other hand, content providers often impose conditions that are unfair and in many cases unacceptable for consumers.

Lars Grøndal from BEUC on secondment from the Consumer Council of Norway, talked about standard terms of contracts regulating how consumers can use digital products legally, and DRM controlling how consumers can use digital content de facto, and the two not meeting in many cases. With a case study on iTunes' standard terms he illustrated how unfair terms and conditions of purchase can be. Grøndal mentioned that consumers are not in a very bad situation, since for example in Norway, one can legally circumvent DRM measures either to achieve accessibility or to be able to play purchased content on another player. He concluded his speech with the statement that "business interests are not the only that deserve protection" (cf. also Grøndal 2006).

Dr. *Anikó Gyenge* from the Hungarian Ministry of Justice talked about the well-known controversy between copyright law and TPM (technical protection measures). She emphasised that not all of the technical functions can be legally interpreted, therefore not all measures are protected by copyright law. She talked about free use and to what extent DRM restricted legal copyright exemptions. In the end she concluded, that while consumers might be in a not too favourable situation, there is a difference between written law and enforced law: since the regulatory system is hard to interpret in practice, judges in many cases do not apply the code – to the benefit of consumers.

Matthias Spielkamp, editor of iRights.info introduced their project to the workshop participants. He said that they examined the contract terms of three music services available in Germany: iTunes, Musicload and Sony Connect had 33, 18 and 55 pages of usage terms respectively after he copied and pasted them into Word, and corrected their font size and layout. iRights.info, a project funded by the German Ministry of Consumer Protection, provides additional information, since, as Spielkamp pointed out, from these terms and conditions "no one is able to understand what is going on". Fairness, openness, reliability, independence and finding the correct balance between alternatives are their main approach. On their web page consumers can find more than 40 texts on basic aspects of law and usage, and there are news every week. iRights.info follows an interdisciplinary approach and uses current media tools to educate German consumers about their rights regarding digital content and DRM.

Consumer initiatives

Martin Springer, a private contributor to the Digital Media Project, started his presentation with a case study: Every couple of years the soccer leagues make their exclusive license deals with three or four content providers, and thus they force their fans to either accept their new proprietary DRM standard, or stop watching the games. Thus if a football fan in Germany wants to follow his team's matches in national and international games, he needs to subscribe to several service providers and network providers, and spend a lot of money for buying incompatible receivers and to subscribe to unnecessary programme packages. He concluded that the industry uses DRM as a weapon against competitors, trying to lock consumers into a particular DRM scheme and particular business models. Innovative media usages like sharing content among soccer fans from different European countries are impossible. Springer suggested that consumers should get involved in DRM standardization with the goal of creating a standard DRM that is open and acceptable for both consumers and rights holders. He introduced the DMP project (Jeges 2005; Jeges and Kerenyi 2005), in which he works because he intends to defend concepts like privacy and End-user Rights in a DRM standard.

Bodó Balázs, assistant lecturer and researcher from the BUTE Centre for Media Research and Education, introduced the Silent Library Project, a commons-based peer production. First he illustrated with figures, that both on the Hungarian, and US markets, considering both books and feature films, around 20 per cent of the titles that have been published within the last 15 years are still available for purchase. The simple reason is lack of shelf space, he said. However, there is still a considerable market demand for those titles not on the shelves. Each is under copyright, but they are not available from legal sources. The Silent Library Project is an illegal movement, a group of people who started scanning and digitizing such titles, and sharing them with each other, making them available again. DRM has a completely different approach, he said: by centralization and access hierarchy they tend to re-create scarcity in the digital world, similarly to the physical world. Bodó illustrated the world in 2050 with an imagined scenario, where all works from 2010 will probably be available secured by unbreakable DRM. In this world, when no marketing is behind a product (it is not in the 20 percent), and commons-based networks (like SLP) are shut down, our knowledge, our common experience will shrink. Culture is a common good – he finished his talk.

Bottom line

Zoltán Hornák, INDICARE project member from SEARCH concluded the day. Since the workshop moved along different stream, each related to consumer aspects, the conclusions he drew from the whole day's presentations and programme were rather diverse.

From the surveys we can learn that there is a clear demand from consumers to obtain content, even paid content, however, if consumers consider the offerings unfair, they will not go with them, and choose alternative channels. Furthermore, consumer expectations of traditional usages must be supported to create viable DRM systems.

In the accessibility session we could learn about the difficulties that blind or other disabled people may face when accessing even unprotected content, and also the controversies of DRM and accessibility. And although nowadays accessibility of content and DRM can work together, we must take care that in the digital world, a world that we can design from the basics, we do not recreate the barriers that are present for some people in the physical world.

The content providers emphasised that DRM helps them to know their consumer and create new business models, while consumer rights experts doubted this statement. From the rights session we learned that consumers are not in a very bad position after all, because in some countries doing "things in the grey", like downloading or freeing DRM-protected content is not illegal according to law, and even if it is forbidden, if judges do not enforce it, code does not have much effect. In any case, informing consumers about rights in a clear and understandable manner is a very important issue.

At the end of the workshop we could hear about two consumer initiatives, one of which tried to work out a better, interoperable and thus for the consumers more acceptable, DRM system, and the other completely rejected DRM and tried to create an (under)world without DRM.

My personal conclusion from the workshop was: consumers, and their wishes must not be neglected any more!

Sources

- Dufft, Nicole, et. al. (2005): Digital music and DRM – Results from an European consumer survey. http://www.indicare.org/tiki-download_file.php?fileId=110
- Dufft, Nicole et. al. (2006): Digital video usage and DRM – Results from a European consumer survey. http://www.indicare.org/tiki-download_file.php?fileId=170
- Grøndal, Lars (2006): DRM and contract terms. INDICARE Monitor, Vol. 2, Number 12, February 2006; http://www.indicare.org/tiki-read_article.php?articleId=177
- Jeges, Ernő (2005): Digital Media Project – Part I. Towards an interoperable DRM platform. INDICARE Monitor, Vol. 2, No 4, June 2005 ; http://www.indicare.org/tiki-read_article.php?articleId=116
- Jeges, Ernő; Kerényi, Kristóf (2005): Digital Media Project – Part II: Chances of an open standard. INDICARE Monitor, Vol. 2, No 6, August 2005; http://www.indicare.org/tiki-read_article.php?articleId=134
- Kerényi, Kristóf (2005): Online music in Hungary. INDICARE Monitor, Vol. 2, No 7, September 2005; http://www.indicare.org/tiki-read_article.php?articleId=138

About the author: *Kristóf Kerényi* is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His interests include mobile and wireless IT security, as well as technological aspects of DRM. He received a MSc in computer science from BUTE. Contact: kerenyi@mit.bme.hu

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=182

DRM and contract terms

By: Lars Grøndal, BEUC, Brussels, Belgium

Abstract: In every day life consumers are frequently accepting standardised contractual and technological terms that they have little or no understanding of. Some of these terms are generally unfair and do not stand up to legal scrutiny. In this article iTunes Music Store's Terms of Service is used as an example of a standard contract containing unfair terms.

Keywords: legal analysis, case study – consumer expectations, consumer protection, music markets, standard contracts, unfair terms

Introduction

Standard contracts are written terms that regulate how consumers legally can use purchased products. DRMs on the other hand are technical measures that control how consumers *de facto* can make use of digital goods and services. Amongst other things, DRMs frequently enforce standard contract terms.

Both DRMs and standard terms are seldom open to individual negotiation – either the consumer accepts them or the consumer will have to take its business elsewhere. If consumers had a wide variety of easily comparable terms this would not be a problem. But as the situation is today, with opaque and often standardised conditions, consumers are facing insurmountable difficulties in obtaining fair terms. Even the legally trained consumer will have trouble getting a proper understanding of all the terms you meet in every day life.

Just like other business practises, standard terms and DRMs do not always stand up to legal scrutiny. In this article I will focus on DRM and contract terms consumers meet when purchasing music online. More specifically, I will look at some of the terms in iTunes Music Store (iTMS, iTunes) Terms of Service (ToS).

At the outset I would like to emphasise that these terms are not unique to iTunes. There are many other digital products where similar conditions apply: software, videogames, CDs, DVDs, etc.

A number of provisions in the iTMS Terms of Service are questionable both in relation to community and national law. I will focus on three terms which are of particular interest in relation to DRM:

- iTMS ability to unilaterally change terms and conditions,
- The limitations on liability, and
- The limitations on interoperability.

Unilaterally change terms and conditions

According to iTunes Music Store Terms of Service, Apple reserves the right, at its sole discretion, to change the way customers can use downloaded material (iTMS 2006).

It says in article 20 that:

> "iTunes reserves the right, at any time and from time to time, to update, revise, supplement, and otherwise modify this Agreement and to impose new or additional rules, policies, terms, or conditions on your use of the Service."

Furthermore, in article 9d it says that:

> "[Y]ou acknowledge that you may no longer be able to use Products to the same extent as prior to such change or discontinuation [...]."

This entails that Apple reserves the right to unilaterally change the way a file can be used after the purchase. For instance, Apple could limit the number of times an iTMS file can be burned onto a CD. If you buy a music file on iTMS today you can burn a playlist 7 times. According to the ToS, Apple is entitled to limit the number of playlist you can burn from the same file tomorrow.

Amendments in the terms and conditions can be enforced by changing the DRM.

A study by Intertek (2005) found that although it would be technically challenging, it is possible to change the DRM on already downloaded material. Boing Boing, a tech news site, reported last year that iTunes Music Store has changed customers' usage rights to material customers already had on their computer (Boing Boing 2005). By installing updates to the iTMS software, customers lost the ability to:

- stream unlimited over the local network (down to 5 times per 24 hours),
- stream over the internet,
- burn a playlist 10 times (down to 7).

Changes might not be enforced by changing the DRM, but simply by amending the Terms of Use. According to the legal terms:

> "It is your responsibility to check these Terms of Use periodically for changes."

If a costumer uses the file in a way which was allowed at the time of purchase, but is no longer permitted, the consumer is in breach of contract. The Terms of Service sets out a range of sanctions which iTMS can apply as they see fit.

Article 14a of the terms state that:

> "If you fail, or iTunes suspects that you have failed, to comply with any of the provisions of this Agreement, […] iTunes, *at its sole discretion*, *without notice to you may* [my italics]: (i) terminate this Agreement and/or your Account […]; and/or (ii) terminate the license to the software; and/or (iii) preclude access to the Service (or any part thereof)."

This entails that the customer could be banned from iTMS at Apples sole discretion and without notice just because she failed to keep herself regularly updated on the Terms of Use.

The right to unilaterally change terms of contract is considered an unfair term according to Directive 93/13/EC (EU 1993) on unfair terms in consumer contracts. Consumers do not expect new terms and conditions being applied retroactively; if you buy a product today and you can use it in certain ways, you expect that you will be able to use the product in the same way tomorrow.

In the annex to the Unfair Terms Directive there is a non-exhaustive list of terms which may be regarded as unfair. Letter j is of particular interest here:

> "enabling the seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract;"

Limitations on liability

Recent examples have shown that DRM systems can cause severe security risks. The copy-protection technology that has been used on some Sony BMG CDs, XCP, left consumers' computers open to attacks (for more information on XCP see EFF 2006).

According to another tech news site, The Register, serious security flaws have recently been discovered in iTMS (Leyden 2006). iTunes Music Store, through its conditions, disclaims all liability for attacks on consumers' computers, even if it is caused by security flaws in Apples DRM, Fairplay.

Article 18a (ii) of the Terms of Service says that:

> "iTUNES DOES NOT REPRESENT OR GUARANTEE THAT THE SERVICE WILL BE FREE FROM LOSS, CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, OR OTHER SECURITY INTRUSION, AND iTUNES DISCLAIMS ANY LIABILITY RELATING THERETO." [The paragraph is for some reason all in capital letters in the iTMS Terms of Service].

This type of term is not specifically mentioned in the annex to the Unfair Terms Directive, but the list is not exhaustive. Consumer protection legislation in many Member States (the Nordic countries for instance) prohibit limitations on consumers' statutory right to damages.

Pursuant to the Norwegian Consumer Contract Act (2001) section 33, vendors are liable for damages caused by the purchased

product. Contractual limitations on consumers' right to damages are void. This law is not directly applicable when downloading music, but it is indicative of the fairness of the term. Consequently, this term should be considered unfair under the Unfair terms Directive.

Interoperability

Fairplay, the DRM used by iTMS, prevents the consumer from using other players than Apple's iPod to play music purchased from iTunes.

The contract also limits which players can be used. Article 9 b states that:

> "You shall be authorized to use the Products on up to five *iTunes-authorised devices* [my italics] at any time. […] You shall be able to store Products from up to five different Accounts on *certain devices, such as an iPod* [my italics], at a time."

The only portable player authorised by Fairplay is iPod. Thus, the contract only allows consumers to use iPod to play files downloaded from iTunes.

Consumers can easily get around this limitation. As the test (Intertek 2005) commissioned by BEUC shows, Fairplay can be erased and the file converted to MP3 format by burning a CD with iTunes files and then subsequently ripping them back to the computer.

If a consumer uses this method to make use of a different player, e.g. a Creative player, this would not be in accordance with the contract.

Tying the consumer to use a certain player, however, can be contrary to community and national legislation. Consumer law, competition law and even copyright law can be used to combat this type of business practise.

It has been discussed whether iTune's refusal to licence Fairplay to competitors could constitute an abuse of dominance contrary to article 82 of the EC Treaty. This is doubtful however; both because of the difficulty in establishing dominance and because of the European Court of Justice' reluctance to impose mandatory licensing (see Reckon 2006).

Consumer protection rules could be an easier option. One could argue that contractual obligations tying iTunes customers to one specific portable player is unfair pursuant to the Unfair Terms Directive.

A French consumer group, UFC Que Choisir, has initiated legal proceedings against Apple, claiming that tying iTunes customers to use iPod and vice versa, is not in accordance with the French consumer code article 122 which says that:

> "It is prohibited to refuse to sell a product, or supply a service, to a consumer without a legitimate reason, and to make the sale of a product subject to the purchase of a minimum quantity, or to the accompanying purchase of another product, or another service, as well as making the provision of a service subject to provision of another service, or to the purchase of a product."

Depending on national legislation, copyright law itself can be used to combat the lack of interoperability. Take for instance the Norwegian Copyright Act that implements Directive 2001/29/EC (the Copyright Directive). Circumventing effective technological measures is prohibited under section 53a of the Copyright Act. In the third paragraph there is an exception to the anti circumvention provision: effective technological measures can be circumvented to play legally acquired works on relevant players. According to some commentators this provision gives consumers the right to circumvent Fairplay in order to use other portable players than iPods (Vigmostad 2005). The Norwegian Consumer Ombudsman has consistently held that standard contractual terms limiting consumers' statutory rights are unfair and void under the Norwegian Marketing Control Act (1972) section 9a .

A different question is whether Fairplay is protected under the Norwegian Copyright Act or the Copyright Directive at all. Both section 53a and article 6 of the Copyright Directive only protects *effective* technologi-

cal measures. In the preparatory works to the Copyright Act, copy-protection on CDs that could be erased by simply writing with a pen on it was characterised as an ineffective protection measures. The copy-protection technology on files downloaded from iTunes is erased simply by burning a playlist. This is very easy to do and is permitted under the contract.

Having said that, making it easy to get around DRMs, and especially those that curtail competition, is a definitively a good thing for consumers and I would not like to see a more effective DRM being implemented in the future.

How do we deal with these kinds of terms?

The Unfair Terms Directive article 7 obliges Member States and other parties to the EEA (European Economic Area) agreement to have "adequate and effective means […] to prevent the continued use of unfair terms".

In the next paragraph of the article it says:

> "The means referred to in paragraph 1 shall include provisions whereby persons or organizations […] may take action according to the national law concerned before the courts or before competent administrative bodies […] to prevent the continued use of such terms".

In Norway the Consumer Ombudsman deals with unfair contract terms. According to the Marketing Control Act Section 9a:

> "Terms and conditions which are applied or are intended to be applied in the conduct of business with consumers can be prohibited if the terms and conditions are considered unfair".

Terms and conditions can mean both traditional written terms, but also technical ones like DRMs.

The Consumer Council of Norway has complained to the Consumer Ombudsman in order to get iTunes terms amended. The Consumer Council has also argued that certain aspects of the DRM Fairplay are unfair and should be amended (Consumer Council of Norway 2006; see also Singstad 2006)

Bottom line

To conclude, there are ways of combating the unfair use of DRMs with today's legislation. However, the current legal regime does not fully take into account the unique characteristics of digital products. European and national consumer legislation focuses mainly on traditional tangible products bought in traditional ways.

Also, the Community legislation being proposed and adopted in this area predominately caters to business interests and does not take into consideration the dire consequences for consumers. Take for instance the Commission's proposal on harmonisation of criminal measures on IPR infringements (EU 2005). According to article 3 of the proposal, intentional infringements of IPRs on a "commercial scale" must be treated as criminal offences. One of the justifications of the proposal was that the "[i]ncreasing use of the Internet enables pirated products to be distributed instantly around the globe". The Directive does not require a profit motive to apply. Thus, it seems that illegal file-sharing through P2P networks are covered by the Directive. Consequently, the proposal can potentially criminalise the technologically proficient youth of Europe. The Commission withdrew the original proposal for competency reasons. To our knowledge the Directive will be reissued in March without substantial amendments. For other examples of EU IPR initiatives where consumer considerations are absent, see Kutterer 2005.

As a response to the lack of public interest considerations in EU policy on IPR, BEUC launched a campaign for consumers' digital rights in November 2005 (BEUC 2005). We believe that business interests are not the only ones which deserve protection in the digital environment. Our aim with the campaign is to raise awareness in this field both among policymakers and consumers and to promote a better legal framework for consumers.

Sources

- BEUC (2005): consumers digital rights: http://www.consumersdigitalrights.org/cms/index_en.php
- Boing Boing (March 16, 2005): Apple steals iTunes customers' paid-for rights to stream http://www.boingboing.net/2005/03/16/apple_steals_itunes_.html
- Consumer Council of Norway (2006): Complaint against iTunes Music Store; http://forbrukerportalen.no/filer/Complaint%20against%20iTunes%20Music%20Store.pdf
- Electronic Frontier Foundation (EFF) (2006): Sony BMG Litigation Info; http://www.eff.org/IP/DRM/Sony-BMG/
- EU (1993): Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Official Journal L 095, 21.4.1993, pp. 29-34; http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31993L0013&model=guichett
- EU (2005): Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights 2005/0127(COD), http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0276en01.pdf
- European Court of Justice (2004): Judgment of the Court (Fifth Chamber) of 29 April 2004, IMS Health GmbH & Co. OHG v NDC, C-418/01
- French consumer code: Article L122-1: http://195.83.177.9/code/liste.phtml?lang=uk&c=61&r=2133
- Intertek Research & Performance Testing (2005): Online Music Download Services. Technical Report 63028 Issue 2, September 2005; http://www.consumersdigitalrights.org/mdoc/OnlineMusicDownloadServices_TechnicalReport_90041.pdfi
- iTunes Music Store (iTMS) (2006): Terms of Service and legal terms http://www.apple.com/uk/support/itunes/legal/terms.html and http://www.apple.com/legal/terms/site.html
- Kutterer (2005): Some of the reasons for BEUC's Campaign on Consumers' Digital Rights. INDICARE Monitor, Vol. 2, Number 10, December 2005; http://www.indicare.org/tiki-read_article.php?articleId=162
- Leyden, John (2006): Apple bitten by iTunes security bugs. The Register Wednesday 11th January 2006; http://www.theregister.com/2006/01/11/itunes_vulns/
- Norwegian Consumer Contract Act (2001): http://www.lovdata.no/all/nl-20020621-034.html
- Reckon LLP (ed.) (2006): iTunes, DRM and competition law. Reckon Open; http://www.reckon.co.uk/open/iTunes
- Singstad, Jo (2006): iTunes' questionable terms and conditions; http://forbrukerportalen.no/Artikler/2006/1138119849.71
- Vigmostad, Tobias (2005): Digital Rights Management Systems as they apply to the Norwegian Intellectual Property Act, Section 53a, Paragraphs 1 and 3, 2nd Sentence; http://www.dagbladet.no/download/oppgave.doc and http://www.dagbladet.no/kultur/2006/02/01/456502.html
- The Norwegian Marketing Control Act (1972): http://www.forbrukerombudet.no/index.gan?id=706&subid=0

About the author: *Lars Grøndal* is a legal advisor currently working for BEUC, the European Consumers' Organisation. He is on a secondment from the Norwegian member, The Consumer Council of Norway. Contact: lars.grondal@beuc.org or lars.grondal@forbrukerradet.no

Status: first posted 23/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=177

Copyright law as an enigma for laypersons and the need for iRights.info

By: Matthias Spielkamp, iRights.info, Berlin, Gemany

Abstract: Implementation of the European Union Copyright Directive's provisions into member states' laws has led to increased confusion about copyright issues for consumers. This is particularly relevant at a time when more and more uses of digital media are regulated by copyright. Rights holders, especially large, multi-national companies, are not willing to inform consumers unbiased. Hence the continued need for publicly funded, impartial consumer information, preferably on a multi-national, multi-language EU level.

Keywords: case study – file sharing, copyright law, EUCD, consumer information, piracy

Why confusion about copyright law is a consumer issue

Five years ago, the European Union's Copyright Directive (EUCD) finally, after four years of negotiations, passed the EU's legislative process. Since then, almost all EU member states have devised and adopted laws to – more or less – implement the directive's provisions into their respective authors rights or copyright codes (with the exception of France, Spain and the Czech Republic). Following its approval by the Council of Ministers, the chairman of the European Commission's Legal Advisory Board Taskforce on Intellectual Property – among many others – criticised the EUCD for its ambiguity: "It does not increase 'legal certainty', a goal repeatedly stated in the Directive's Recitals (…), but instead creates new uncertainties by using vague and in places almost unintelligible language"(Hugenholtz 2000). In the case of Germany, these new uncertainties have carried over into the country's revised authors rights code, which came into effect in September 2003. To give an illustration of what this entails for regular users of digital media and the Internet, I will first provide a case study of the legal implications of file sharing in Germany. I will then briefly explain the role of the iRights.info (cf. sources) as a consumer information portal on copyright issues.

Case study: File-sharing and the law in Germany

Many uses of file-sharing networks are completely legal. Some people know this, some may take it for granted, but to some people this will sound rather surprising. Reading newspaper articles on the topic or watching TV reports, one can certainly get the impression that everything that has to do with file-sharing is so called "illegal piracy". But this is not the case.

Sharing someone's own works – texts, music, pictures, videos, software, games, animations and so on – is completely legal. Or, to be more specific: It is legal to share works if the person sharing them holds the rights to these works. For example, more and more companies put files on the web to share as well: music for promotional purposes, movie trailers and the like.

In addition to works someone owns, sharing is allowed for works the copyright holder allows to be shared – this sounds obvious, but one has to be aware that the rights holder must specifically assign those rights. This is done quite often, though, i.e. with works under Creative Commons licences (cf. sources), the GPL (GNU General Public Licence) (cf. sources) and many others.

Then there are works in the public domain. An example for this is the Project Gutenberg (cf. sources), where scholars, students, and activists digitize classical texts from Aristotle to Zola and make them available in a searchable database.

In a majority of cases, file sharing networks are used to break the law

Most uses that are actually practiced on today's file sharing networks are illegal, though. The vast majority of music, films, software, and texts are copyrighted and the

rights holders prohibit sharing. Since the so called "first basket" (first round) of the German copyright revision came into force in September 2003 (Bundesministerium 2003), it is illegal for individuals to make available works in a file-sharing network without holding the rights to them – which is the majority of works on file-sharing networks today. So most of the actual uploading being done is clearly illegal under German law.

Downloading still considered legal in Germany by many

Downloading is a different matter, though. If a user in Germany downloads a song from a file-sharing network, it is seen as a duplication – a copy of the song. If this copy is for private use, it is perfectly legal – like copying a CD or a videotape. This permission is granted by an exception to copyright ("Schrankenregelung"), resembling – not equalling – the fair use provision in US copyright law. Of course it is not allowed to sell or lend this copy, because then it would be a commercial use, which is prohibited.

But copying for private use is only allowed if the original is lawful; if the work from which the copy is made is itself "evidently an unlawful copy", it is prohibited. But how can someone tell whether it is evident that this work found on the file-sharing network was produced unlawfully?

This question is very hard to answer. Imagine you find a copy of the movie "Independence Day" on the file sharing network Kazaa and decide to download it. Is this lawful?

It might well be. It has been shown on TV in Germany. So someone might have recorded the TV broadcast on his PC and converted the recording into a digital file. With this he is making a copy for private use, which is perfectly lawful. If he put the file on a file-sharing network, though, he would clearly be breaking the law because he doesn't have the right to distribute the movie, or to make it available. But someone downloading the file would not be breaking the law, because it was not evident that the copy that was made available was produced illegally. It was illegal to make it available, but the subsequent copying of the file is legal.

The difference between "Independence Day" and "Walk the Line": obvious or not?

Confusing? Certainly, but it gets even worse. Imagine someone finds a copy of "Walk the Line" on a file-sharing network. Is it legal to download it? As we have seen, it would be, if it were not obvious that the copy found on the network was produced illegally. But is it obvious that it is a copy produced illegally? To answer this question, one has to be able to answer the following questions: Has the movie in question been broadcast on TV? Answer: Probably not, it just came out in Germany, it is a big production and in cinemas at that moment. Has it been released for home viewing?

Answer: This is difficult to determine. It is a rather new movie. But then, US movies are often releeased in the US long before they come to theatres in Europe (i.e., the drama "House of Sand and Fog", which was released in the US on December 26, 2003, came to theatres in Germany on February 17, 2005 – more than a year later. At the time the movie was still showing in German theatres the DVD was already available in the US, where it was released March 30, 2005 (cf. House of Sand and Fog). And if the person planning to download the movie lives in a small city with only one cinema, then she is familiar with the situation that movies come out a lot later there than in Berlin, Madrid, or London. So if it came out in the US a year ago already, it might have been released for home viewing in the US a while ago. Therefore someone could have bought the DVD of the movie, made a private copy of it and put it on the file-sharing network – this way it would be legal to download it.

But what if the DVD is copy-protected? Because of anti-circumvention legislation, it may be illegal to make a copy, even for private use. For one, all these laws are very complicated to understand and interpret, even for legal professionals. Additionally, how would a downloader know whether "Walk the Line" is copy-protected or not? In our sample case, he does not even know whether it has been released on DVD yet.

So after exhaustive and careful deliberation the user decides to download the movie. By

doing this, he brakes the law – at least that is what the rights holders say. Because "Walk the Line" has not been released for home viewing to date, the file on the file-sharing network has to be a copy someone made with his video camera in a cinema, and therefore illegal. So the user has not only waited for hours for an abysmally bad and grainy copy of "Walk the Line" to download onto his PC, he also has the studios demanding damages.

iRights.info: A continuing effort needed to inform citizens about copyright issues

The example analysed above shows the complexity of the law and, as a result, the difficulty in understanding and interpreting it. This case can only illustrate the situation in Germany, because EU member states' jurisdictions differ widely in the concept of copyright and authors rights codes in general and the implementation of the EUCD in particular. Judging on the basis of media reports from different countries, it can be safely assumed that in many cases their situation is comparable to that in Germany.

To expect rights holders to provide balanced information on copyright issues is futile. Various analyses of their campaigns targeted towards consumers (e.g. Spielkamp 2005; Djordjevic et al. 2005) have shown that their only identifiable interest lies in causing fear, uncertainty and doubt in regard to what rights consumers have using digital media, in order to convey the impression that all uses are subject to permission by rights holders.

Impartial information on copyright issues sought by consumers

In Germany, one approach to mitigate consumers' information deficit is iRights.info , a web site mainly funded by the Ministry for Consumer Protection. INDICARE Monitor readers might already know about iRights by the interview with its legal expert *Till Kreutzer* (Kreutzer 2005). Four part time editors, all specialised on copyright issues in their respective professions (law, art, information science, journalism) compile a wide range of articles illuminating the implications of every day uses of copyrighted works: under what circumstances it is legal to copy CDs, post pictures in your weblog, use samples in your own music, and so on.

The web site currently receives more than 1.500 unique visits per day, showing a high demand for this kind of information. This impression is substantiated by the fact that frequently, people send e-mails to the editors, asking specific questions they do not find answered for in the articles. In these cases, because of legal regulations in Germany, the editors cannot provide legal advice regarding specific cases, but attempt to point to articles and information that should help answer the case in question.

The nature of users' inquiries so far clearly back the stated assumption about the nature of copyright regulation. Most of them show a helplessness regarding the interpretation of the law when it comes to uses of digital media both in situations where people would like to use digital content and when they would like to create new works.

iRights.info as a pan-European project

Funding for iRights.info will run out at the end of March, 2006. As argued above, the notable deficit of this kind of relevant and impartial information about copyright and authors rights issues for consumers remains. iRights.info will therefore attempt to widen the scope of iRight.info to make it a pan-European project and secure funding from the European Union. In case of an interest in cooperating towards this aim, please contact the author at ms@iRights.info.

Sources

- Bundesministerium der Justiz: "Neues Urheberrecht ab morgen in Kraft", http://www.kopien-brauchen-originale.de/enid/5j.html, text of law available at http://217.160.60.235/BGBL/bgbl1f/bgbl103s1774.pdf (accessed February 15, 2006)
- Creative Commons Website, http://creativecommons.org (accessed September 2, 2005)
- Djordjevic, V; Kreutzer, T.; Spielkamp, M.: iRights.info. Informationsgesellschaft und Urheberrecht. Log In 136/37 (2005), pp.118-122
- Free Software Foundation: GNU General Public License, http://www.gnu.org/copyleft/gpl.html. (accessed February 15, 2006)

- Hugenholtz, B.: Why the Copyright Directive is unimportant, and possibly invalid. European intellectual property review (EIPR) 11, 2000; http://www.ivir.nl/publications/hugenholtz/opinion-EIPR.html (accessed February 15, 2006)
- House of Sand and Fog-website: http://www.dreamworks.com/dvd_features_hosaf.html (accessed February 15, 2006)
- iRights.info: http://iRights.info
- Kreutzer, T.: Copyright - complexity - confusion. The basic approach to copyright needs rethinking. INDICARE-Interview by Nicole Dufft. INDICARE Monitor Vol. 2, No 4, 24 June 2005; http://www.indicare.org/tiki-read_article.php?articleId=119
- Project Gutenberg: http://www.gutenberg.org (accessed February 15, 2006)
- Spielkamp, M.: iRights.info. The need for reliable and trustworthy consumer information after copyright revision in Germany. Axmedis 2005, Proceedings of the 1st International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution: Volume for Workshops, Industrial and Applications Sessions, p. 113-118

About the author: *Matthias Spielkamp* is an editor at iRights.info. He publishes in national newspapers, magazines, online publications (Die Zeit, FAZ, SZ, taz, Spiegel ONLINE, Golem.de, telepolis etc.) and his weblog immateriblog.de. He can be contacted at ms@iRights.info.

Status: first posted 23/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=176

Christophe R. vs Warner Music

French court bans private-copying hostile DRM

By: Natali Helberger, IViR, University of Amsterdam, The Netherlands

Abstract: France is one of the European countries where a particularly vivid public discussion about DRM and the private copying exception took place. This is thanks to the efforts of French consumer organisations that initiated a number of court cases dealing with complaints of consumers about CDs and DVDs that could, among others, not be copied and ripped because of technical protection measures in place. This article discusses the latest DRM decision in France, a decision that went one step further than its predecessors when dealing with the difficult question of the relationship between DRM and private copying.

Keywords: legal analysis – consumer expectations, copyright law, court decision, DRMS, EUCD , private copy – France

France developed important body of case law

That there is a conflict between DRM use and consumer interests has been demonstrated over the past three years by the number of cases about CDs and DVDs that could not be played on car radios, PCs and laptops or could not be copied and ripped because of installed technical protection measures. Over the course of three years, French courts have developed the argument that the ability to play a CD or a DVD on different devices, including the radios from different brands of cars or different kinds of computers, constitutes an essential characteristic of a CD or DVD.

Consequently, where phonogram or DVD producers failed to warn consumer about possible incompatibilities between content and consumer hardware, the former could be held liable because of misleading behaviour towards the consumer (Tribunal de Nanterre 2003a, Tribunal de Nanterre 2003b). More complicated, and less promising for consumers, was the situation regarding DRM and private copying. Unforgotten is the finding of The Tribunal Paris in one of the earlier DRM cases in France, that there was no "right to private copying" (Tribunal Paris 2004 – the

"Mulholland Drive" case). This was a black day for the private copying exception. Worse, it delivered the content industry a standard argument which is still regularly evoked by CD and DVD producers when defending their policy of letting the private copying exception die a forceful, electronic death. However, the last word in this matter was not yet spoken, and a year later the Court of Appeals concluded that there may be no right to private copying, still the private copying exception formed a restriction to the exclusive exploitation rights conferred to right holders, and as such was not at the disposition of DRM users (Court of Appeals, Paris 2005).

There was a new decision on 10. January 2006 about DRM and private copying, on which we will report here. The timing of the case, one might want to add, could not have been better: presently pending before the Assemble Nationale, the French Parliament, is the long-overdue proposal for a revised copyright law that implements the provisions of the European Copyright Directive from 2001, including the section on the swelling conflict between technological protection measures and copyright law. The present article will have a closer look at how the Tribunal de Grande Instance de Paris approached the matter. In a subsequent article (Helberger 2006), we will have a closer look at the pending reform of French law and the implementation of the provisions in the European Copyright Directive (EUCD) that is meant to solve the conflict between copyright exceptions and DRM, Article 6 (4) of the European Copyright Directive.

Christophe R., UFC Que Choisir / Warner Music

This latest case involved Christophe R. and UFC Que Choisir against Warner Music France and the music store Fnac. Christophe R. bought a CD by *Phil Collins*, "Testify", to discover later that he could not play it on his laptop, nor could he make copies from the CD. All this, according to Christophe R. and UFC Que Choisir, was because of some form of incorporated electronic copy protection. The plaintiffs' arguments – conflict with the "right to private copying" (since the decision of the Paris Court in 2004, it seems to have become standard among defendants of the consumer side, to refer to a "right to private copying", but then in quotation marks) and misleading behaviour – are familiar from earlier cases (see Tribunal Paris 2004, also Tribunal Bruxelles 2004). And again, the defendants insisted that UFC Que Choisir had no active legitimation to bring the case to court, that a right to private copying was non-existent, that the private copying exception would have to be interpreted in the light of the so-called three step test and, this is a new one, that informing consumers about the fact that burning the CD was impossible was futile as copying technology was in a state of constant flux – how could a decent producer keep track and label his products accordingly?

Thankfully, the Paris Court dealt rather curtly with the argument of a lack of legal standing of UFC Que Choisir (not accepted) and the argument of lack of playability (accepted). It then ventured, without further delay, bravely onto a terrain that causes grown-up politicians and law makers to mumble excuses, look in a different direction or at their shoes and do their best to change the topic. I am speaking of Article 6 (4) of the European Copyright Directive. Article 6 (4) of the European Copyright Directive is the provision in the European Copyright Directive that addresses the conflict between DRM and copyright's exceptions. I say "addresses" and not "solves", because all that Article 6 (4) of the EUCD does is to determine rather vaguely that "Member States shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation … the means of benefiting from that exception or limitation."

Court says: Users of DRM have to respect private copying exception

The Tribunal de Grande Instance Paris, after having defended once again the private copying exception and explaining patiently why it was not in conflict with the three-step-test, stressed the need to interpret French law in the light of the European Directive (see already Court of Appeals, Paris, 2004). The

court's interpretation of Article 6 (4) of the EUCD led it to the conclusion that technological protection measures must respect certain exceptions, including the private copying exception. With the understatement that is so characteristic of French judges, the court then expressed in a few words the essence of much scholarly writing and ranting over the past years by observing matter-of-factly: "the application of anti-copying protection devices by phonogram producers causes the statutory limitations of the authors' exclusive rights to authorise or prohibit reproductions to fade" ("La mesure de protection adoptee par le producteur du phonogramme fait disparaître la limite fixée par le législateur au droit exclusif de auteurs d'autoriser ou d'interdire la reproduction de leurs oeuvres"). Indeed.

The court continued with admirable straightforwardness to conclude that it is task of the DRM user, here: the phonogram producer, to make sure that private copying remains possible, despite the application of technological protection measures. In this point, it differed from the findings of the Court of Appeals in the "Mullholland Drive" case. There, the court did not read a principal obligation for rights holders to observe the private copying exception or any other exception in copyright law in Article 6 (4) of the EUCD. Consequently, the Appeals Court refrained from requiring compliance of DRM and the private copying exception, a matter that the court then left for the legislator. It restricted itself to postulate that 'the complete blocking of any possibilities of making private copies was an impermissible behaviour under French copyright law' (Court of Appeals, Paris 2005). In the Christophe R. case, the court was less hesitant and condemned Music Warner to refrain from using technological protection measures on "Testify" that do not allow for private copying. For each day of failure to comply with the order Warner Music will receive a monetary fine. In this concrete case, the conflict between TPMs and private copying was settled, at least for the time being (note: the case can still go on appeal).

Remains only the question what about all other CDs that are not by *Phil Collins*, produced by Warner Music, bought by Christophe R., called "Testify" and apply private-copying-hostile DRM? The decision of the Tribunal de Grande Instance has binding effect only between the parties immediately concerned. The answer can be read in Article 6 (4) of the EUCD: it is, indeed, up to parliament to settle the conflict.

Bottom line

Until now, France left it to its judges to face frustrated consumers and eloquent industry representatives and to sort out complaints about CDs or DVDs that would not play on a car radio, a PC, a laptop, and/or that could not be copied or ripped. French case law went through different phases: from a "no right to private copying" over explicit invitations to the legislator to take the matter into his hands, up to a ban on DRM that restrict private copying altogether. One thing is for certain: in the end the legislator will have to step in and face the matter. This is already because of the obligation in Article 6 (4) of the European Copyright Directive. So far, the pending proceedings in France to – finally – implement the European Copyright Directive into French law are not too promising. But this is yet another story…

Sources

- Helberger, Natali (2006): Vive la Balance! Pleading for a French revolution of copyright. INDICARE Monitor, Vol. 2, Numer 12, February 2006; http://www.indicare.org/tiki-read_article.php?articleId=181
- Senftleben, M. (2004): Copyright, Limitations and the Three-Step Test, Kluwer International, Den Haag, 2004
- Tribunal de Grande Instance de Nanterre (2003a): Tribunal de Grande Instance de Nenterre 6ème Chambre, judgement du 24 juin 2003, Association CLCV / EMI Muisc France, available at: http://www.legalis.net
- Tribunal de Grande Instance de Nanterre (2003b): Tribunal de Grande Instance de Nanterre 6ème chambre, judgement du 2 Septembre 2003, Francoise M. / EMI Music France, Auchan France, available at: http://www.legalis.net

- Tribunal Paris (2004): Tribunal de Grand Instance de Paris 3ème chambre, 2ème section, Stéphane P., UFC Que Choisir/Société Films Alain Sarde et, Judgement du 30 avril 2004, available at http://www.legalis.net
- Tribunal Bruxelles (2004): Tribunal de première instance de Bruxelles, L'ASBL Association Belge de Consommateurs TestAchats/SE EMI Recorded Muisc Belgium, Sony Music Entertainment (Belgium), SA Universal Music, SA Bertlesmann Music Group Belgium, SA IFPI Belgium, Judgement du 25 mai 2004, No. 2004/46/A du rôle de référes
- Court of Appeals (2005): Coud d'Appel de Paris 4ème chamber, section B, arrêt du 22 avril 2005, Stéphane P., UFC Que Choisir / Universal Pictures Video France et autres, available at: http://www.legalis.net

About the author: *Natali Helberger* is senior project researcher at the Institute for Information Law (IViR), Amsterdam. She specialises in the regulation of converging media- and communications markets, electronic control of access to information and information services and the interface between technique and law, European media and intellectual property law. Ms. Helberger participates in the INIDCARE project as legal partner. Contact: mailto:helberger@ivir.nl

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=180

Vive la Balance!

Pleading for a French revolution of copyright

By: Natali Helberger, IViR, University of Amsterdam, The Netherlands

Abstract: This article reports about the French implementation of the famed Article 6 (4) of the European Copyright Directive, the article that orders member states to guarantee that consumers can benefit from exceptions despite the application of technological protection measures. Considering the fact that France is the origin of a series of groundbreaking decisions in favour of a balance between DRM use and consumer interests, figuring prominently among them the private copying exception, and all the public discussion those cases triggered, we have all reason to be curious about what the French legislator will come up with.

Keywords: legal analysis – copyright law, DRMS, EUCD, private copy, technical protection measures – France

The awkward matter of DRM and copyright exceptions

There are probably few that would not agree that the anti-circumvention rules in the European Copyright Directive (EUCD) are a little tricky, if not to say awkward, or, let's be honest: simply not very well thought-through. Protecting right holders against greedy pirates may be a good and noble cause. Trouble is: the task of the copyright legislator is more complex than that. His task is, on the one hand, to protect and stimulate rights holders and, on the other hand, to promote the broad dissemination and use of works and to protect the public interest in works. Copyright law is a compromise between the economic and moral interests of right holders and public information policy interests in letting all of us benefit from creation and knowledge (Bard and Kurlantzick 1999). Though technological protection measures may, as some argue, benefit right holders in their battle against piracy, the reality is that the way technological measures are applied is often in conflict with cherished and broadly acknowledged principles of copyright law. The private copying exemption is one of these, to name but one, probably the most popular example.

Over the past three years important case law has evolved in France concerning the relationship between DRM users and consumers (cf. Helberger 2004, 2005a, 2005b, 2006).

The French cases also informed lawyers, policy makers and academics outside of France. Having said that, the French decisions are binding only among the parties to the process, and cannot replace a more systematic approach to the conflict between DRM and copyright. To develop the latter is task of the French parliament, as the European Copyright Directive itself already states (in Article 6 (4) of the European Copyright Directive).

Copyright reform in France

As a matter of fact, that is exactly what the French Parliament is trying to do these months, in project Dadvsi (Le Project de Loi (N° 1206) relatif au droit d'auteur et aux droits voisins dans la société de l'information). Project Dadvsi serves the long-pending implementation of the EUCD, including, of course, the provisions about technological measures. Project Dadvsi took an interesting turn. Originally, the project was clearly destined to boost the legal position of the content industry, with proposals for the extensive protection of technological measures, draconic fines for file-sharers (jail up to three years), restrictions on the use of free software, mandatory obligations to implement DRM à la broadcasting flag, etc. Much to the horror of Minister of Culture Renaud Donnedieu de Vabres, the project then changed under the influence of massive external protests and some obstinate parliamentarians (socialists, who else) into a passionate discussion about guarantees for the private copy, legalising p2p networks and making interoperability of DRM mandatory. About 200 suggested amendments and lengthy heated discussions thwarted his initial plan to pass the law quietly and peacefully around Christmas 2005. Amendments suggested included interesting proposals like that technological protection measures should only be implemented with the knowledge/authorisation of the original author of that work (Amendment No. 84) or the suggestion to guarantee the private copying exception (Amendments No. 153 and 154). It remains to be seen which of these amendments will make it into the final bill. It would lead too far to discuss in this article all amendments, instead, we will concentrate on the transposition of the infamous Article 6 (4) EUCD in Article 8 of the draft law.

A French DRM-sarabande: One step to the front, five steps back

Article 8 of the draft law basically states that right holders will take initiatives to allow users to benefit from a private copying exception or an exception in favour of disabled persons. The rest of the draft article then concentrates on listing limitations to this obligation:

1. This only applies to consumers that have rightful access to the work (a provision that stems from the EUCD).
2. The obligation only applies in case the exception does not conflict with normal exploitation interests or legitimate interests of the author.
3. The right holder, furthermore, has the possibility to restrict the number of copies allowed.
4. The obligation does not apply to works that are made available on demand and at individual request, thereby excluding all download online services such as iTunes, movielink, etc…
5. And, finally, it is difficult to see how the obligation could be effective.

Why the present approach is a farce

The French legislator made the lion warden of the sheep. Admittedly, it seems a logical and fair step to burden users of DRM with the responsibility to make sure that the technology is applied in a way that respects the existing legal order. This was also the finding of the Tribunal the Grand Instance Paris. Having said this, any such obligation is of little value without accompanying measures that guarantee its enforcement (interesting, for the field of environmental law, see Börkey, P.; Glachant, M; Lévêque, F. 1998). Where the court imposed at least a daily fine in case of non-conformity, the draft law leaves a blank void. There is no deadline for the transition towards exception-friendly DRM, except a hazy rule that such initiatives would have to be taken "with a reasonable delay". Neither does the draft law foresee an independent body that would supervise the

value and success of such initiatives to make DRM more exception-friendly. A vague reference is given that initiatives are made in agreement with interested parties. It is unclear who these interested parties are, if they must include representatives of consumer or public interests, what influence interested parties actually do have to bring in their interests effectively, etc.

Neither does Article 8 stipulate what shall happen if DRM users do not obey. According to the present draft: nothing. In the worst case, frustrated beneficiaries could take their case before the new arbitration body (that is to be created according to Article 9 of the draft law). The arbitration body can order DRM users to undertake initiatives necessary to benefit from an exception. Insofar, Article 9 of the French draft law resembles e.g. the Danish solution of a Copyright Tribunal (in § 75 d (1) of the Danish Copyright Act) (as to possible problems with this solution, see Foged 2004). Unclear is whether consumers (and consumer organizations) will still be able to bring DRM cases before courts, or whether they will in future have to file their complaints with the arbitration board first. In the latter case, the draft proposal might effectively set an end to a slowly but surely emerging body of case law in favor of consumer interests and DRM in France.

Equally problematic is the tendency that is expressed in the French draft as well as in the EUCD to protect the existence of exceptions in the offline environment, while accepting that they are overridden by technological measures and contracts in the online environment. It is difficult to see why the exceptions and limitations of copyright law should not apply in the online world. This is a technology-dependent approach that is likely to fail completely in the age of convergence. The fact that the danger of abuse is, as the argument goes, higher in an online environment does not alter the basic considerations about cultural exchange, freedom of expression, personal autonomy, information equality, etc. that have motivated the exceptions in the first place.

And even for the offline environment, the French draft law basically issues a charter to DRM users to override existing exceptions and limitations except the two mentioned in the draft Article 8: private copying and exceptions in favour of disabled persons. Why these two? In the public discussion around DRM and copyright exceptions, those are the ones discussed most loudly and that have, hence, the most political explosive potential. This, however, also demonstrates the danger of a too narrow discussion about DRM: important interests of the press, of artists, of libraries, universities and social institutions are too easily overlooked. For the protocol: the DRM-and-consumer-debate is not only about CDs and DVDs and private copying. It is about all kinds of digital content – text, news articles, books, games, film on or offline – and the various and diverse interests attached to its creation and dissemination.

It would seem that the Ministry of Culture is persistently trying to turn a deaf ear to the noise on French streets and in French courts. But France is in the national and international spot-lights: now is the time to act and to solve the conflict between DRM and copyright exceptions! Vive la balance!

Bottom line

Do we expect too much from France – every 217 years a new revolution (cf. Imhof 2005)? No, not at all. Over the past few years and thanks to the efforts of French consumer representatives, a public discussion has developed in France about DRM and consumers. This is a discussion that has influenced the way to look at DRM far beyond the borders of France. Creating the conditions for a more consumer-friendly DRM environment is not revolutionary – it is an increasingly widely acknowledged necessity for the functioning of the information society.

The basic approach being discussed presently in France in courts and parliaments – to hold DRM users liable for compliance with the law – is a hesitant step in the right direction. Liability alone however is not enough. Such an approach must be accompanied by measures that guarantee that DRM users take timely initiatives, and that such initiatives are effective and reflect the interests of all parties, including those of consumers.

Sources

- Bard, R. and Kurlantzick, L. (1999): Copyright Duration. Duration, Term Extension, The European Union and the Making of Copyrigth Policy, Austin & Winfield Publishers, San Francisco, 1999
- Börkey, P.; Glachant, M; Lévêque, F. (1998): Voluntary Approaches for Environmental Policy in OEDC Countries: An Assessment, online available at http://www.cerna.ensmp.fr/Documents/PBMGFL-OECDVAs.pdf
- Helberger, N. (2004): It's not a right, silly. The private copying exception in practice, INDICARE Monitor Vol. 1, No 5, 29 October 2004, available at: http://indicare.berlecon.de/tiki-read_article.php?articleId=48
- Helberger, N. (2005a): Thou shalt not mislead thy customer! INDICARE Monitor, Vol. 1, No 9, 25 Feb-February 2005, available at: http://www.indicare.org/tiki-read_article.php?articleId=76
- Helberger, N. (2005b): Not so silly after all - new hope for private copying, INDICARE Monitor, Vol. 2, No 6, 26 August 2005, available at: http://www.indicare.org/tiki-read_article.php?articleId=132
- Helberger, N (2006): Christophe R. vs Warner Music: French court bans private-copying hostile DRM. INDICARE Monitor, Vol. 2, Numer 12, February 2006; http://www.indicare.org/tiki-read_article.php?articleId=180
- Foged, T. (2004), Overview of implementation of the European anti-circumvention rules in Denmark, available at: http://www.euro-copyrights.org/index/4/11
- Imhof, P. (2005): Neues Urheberrecht in Frankreich, blog, 22. December 2005, available at: http://fippu.ch/)
- Le Project de Loi (N° 1206) relatif au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI), available at: http:// http://www.assemblee-nationale.fr/12/dossiers/031206.asp

About the author: *Natali Helberger* is senior project researcher at the Institute for Information Law (IViR), Amsterdam. She specialises in the regulation of converging media- and communications markets, electronic control of access to information and information services and the interface between technique and law, European media and intellectual property law. Ms. Helberger participates in the INIDCARE project as legal partner. Contact: helberger@ivir.nl

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=181

DRM beyond copyright enforcement

Alternative models for content distribution

By: Daniel A. Nagy, Search-Lab, Budapest, Hungary

Abstract: In this article, we propose an alternative content distribution framework, which provides the necessary incentives for creating digital content without resorting to copyright enforcement. The proposed business model relies on peer-to-peer digital payment for which technical solutions already exist. Existing DRM technologies may actually be recycled for the purposes of the proposed business model, while removing the incentive misalignments currently plaguing the industry.

Keywords: economic analysis – business models, e-payment, DRMS, media markets, P2P

Introduction

DRM (Digital Rights Management) has traditionally been thought of as a tool to enforce copyright. As such, it has failed spectacularly on several occasions (see e.g. Rubens 2002 about the DVD region code debacle or Orlowsky 2004 about the defeating of iTunes DRM). Practically every DRM solution with wide enough deployment for people to care was defeated within a short period of time.

In this article, we propose alternative business models which would provide the par-

ticipating parties with the right incentives to do what other participants expect them to do, irrespectively whether or not copyright is enforced.

The proposed business models are based on several already successful business practices, which encourage creativity without relying on copyright protection. We strive to eliminate or minimize externalities by making sure that every participant is paid exactly for what they provide and pay exactly for what they get, while remaining in full control of whether or not to sell or buy services at a given price and are aware of the available alternative choices. Thus, the proposed business models can be expected to fare well in an unregulated free market.

Why does DRM fail as a tool of copyright enforcement?

The reason for this is that DRM is marred with severely misaligned interests of the concerned players:

1. Content authors, whose interests include compensation for their work, a loyal audience and wide publicity;
2. Publishers/distributors, whose primary interest is high revenue from content distribution;
3. Consumer electronics manufacturers, whose primary interest is high revenue from sales of devices;
4. Consumers, whose interests include low prices and a wide assortment of available content;
5. Governments, whose interests include high tax revenues, low enforcement costs, a reputation for enforcing laws and popular support.

DRM, in its traditional role as a tool of copyright enforcement, requires cooperation between authors, manufacturers, governments and publishers. In the light of the fact that devices with easily defeatable DRM sell better in an unregulated market, while implementing secure DRM is expensive, manufacturers need additional incentives to cooperate, such as government intervention and/or exclusive contracts (or even merger) with publishers/distributors. Also, manufacturers may choose to relocate to countries where such government intervention is smaller, thus providing governments with an incentive to defect from this cooperation. In addition, cooperation in copyright enforcement may erode the popularity of content creators, manufacturers and governments alike. The recent Sony-BMG case is an illustrative example of such backlash.

In such an environment, enforcing copyright in the face of extremely cheap, high quality alternative distribution channels (such as digital networks and recordable media) is a very difficult undertaking. On the other hand, content consumers have every reason to cooperate *against* copyright enforcement and can do so quite successfully, as has been observed with the widespread practice of burning CDs and DVDs for one another and the popularity of and considerable engineering effort put into peer-to-peer file-sharing and defeating DRM solutions.

For what are consumers prepared to pay?

As witnessed by the popularity of the otherwise quite expensive call-in and SMS votes on interactive television (such as those on Music Box, MTV and other commercial television channels), content consumers are prepared to pay for seeing their favourite content rank high in popularity ratings.

Such voting systems typically allow for multiple votes, precisely because voting requires financial sacrifice on the part of the voter, thus multiple voting is indeed indicative of higher commitment.

There is also evidence (see e.g. Madden 2004 about how artists perceive the issue) that consumers are quite willing to pay the author directly, even if the content is available for free from other sources. The more intermediaries are between the audience and the author, the more reluctant the former become to pay, if there are other means to get hold of the content.

Without going into moral or legal arguments, several surveys and other research suggest (see e.g. Madden 2004 and Dufft 2005) that the overwhelming majority of music consumers and authors (in sharp contrast with publishers) do not consider file-sharing as a

major threat to the creative community. Most, however, do think that authors should be compensated.

Thus, it is reasonable to assume that people would be even more willing to pay for expressing their support for their favourite artists, knowing that most or all of the money they pay will go directly to the artist.

As recently as December, 2005, *Matt Philips* from the British Phonographic Industry (BPI) stated the following in an interview to BBC: "Download services would be far more popular if we gave all the music away for free. But of course we wouldn't have a business then – it's important that you charge for the product and that money can be re-invested in discovering new talent."

In the next section, we hope to address Mr. Philips' concerns in an innovative way.

Solutions for collecting and allocating such payments

Imagine a digital marketplace (e.g. a web- or mobile-portal) for content, where authors can offer their content, possibly with a short description and free samples for download in exchange for payment. All the payment is collected on accounts tied to corresponding pieces of content. There are no restrictions as to how much consumers can pay, except, perhaps a minimum price set by the author.

Content for sale is ranked according to the amount of money on these collector accounts. Thus, paying is essentially voting, informing other consumers about the popularity of the content. Authors can withdraw money from their accounts up to the accumulated balance. Thus, if they wish so, they can receive all the money their supporters paid. Alternatively, they can leave enough on the account to maintain or achieve high ranking.

In this model, the operators of such marketplaces are paid for exactly what they provide: discovering and evaluating talent. By being able to use the money left by authors on the collecting accounts, they essentially get access to interest-free credit. From their point of view, they get to sell their service at an auction price, which is the most they can hope for in a free market.

It is important to emphasize that ranking high does not directly increase or decrease the amount of money paid by supporters. We believe that the argument made in Fortunato (2005) applies to our system as well, which thus actually helps lesser known content providers (e.g. young artists) to attract attention and funding.

While, from a theoretical point of view, the proposed system works with unprotected content, DRM techniques can aid this business model by reducing the load on the operator; the operator in this case can sell only the rights, while the encrypted content itself is available for download from elsewhere, including peer-to-peer networks. In this case, DRM is not critical. If the minimal amount for getting the rights is lower than the effort required for defeating DRM, there is little motivation to attack it.

Another business model, which can even coexist with the previous one, is when customers are allowed to re-sell the content they have purchased at any price and in any quantity. In this case, the price customers will be willing to pay is considerably more than that of enjoying the content and voting for the artist; as it also includes the anticipated income from re-selling the content. Buyers who are also prospective sellers are interested in excluding free-riders, but protecting potentially very large files on storage and during transmission can be expensive. This is another point where DRM solutions can aid this business model: the content itself is available in encrypted form on web servers and peer-to-peer networks, but rights, including the decryption keys, are traded for money. Of course, the price will keep falling, but until it reaches a low level when protecting the content from non-paying consumers is not worth it any more, access to content will be kept restricted by those already accessing it. An extensive analysis of such a market is provided by Boldrin and Levine in their 2005 paper.

In both cases, it is instrumental to keep transaction costs as low as possible, as the transaction values on many occasions are very low. Both cash-like digital currencies with easy peer-to-peer payment and DRM solu-

tions with small rights files enabling the use of large content files help reducing transaction costs to the point where the above outlined business models become viable.

Discussion

The proposed models are by no means restricted to music. The primary criteria for the applicability of the two proposed solutions are the following.

In the case, where payment also constitutes a vote for the content, the applicability depends on how the reputation of the author influences the demand for current and future work by the same author. It is an interesting question, whether or not such a system favours already popular content. While intuitively one would think that the proposed ranking scheme is biased against lesser-known authors and their works, such intuition is not necessarily justified (see Fortunato 2005 for a similar example). For instance, in an ordered list the difference between the attractiveness of the first and the second placed items does not directly depend on the actual difference between the amount of collected (and unused) funds. Another possible objection is that the proposed funding scheme does little to help the emerging artist to recoup the significant upfront costs of production. We believe that this is primarily a question of credit and the proposed system can be relied upon as a source of re-paying such credit. Furthermore, it allows the customers to credit the author directly, assessing the creditworthiness on the basis of past work.

In the second case, when content can be traded freely, the essential element for making the market efficient from both authors' and consumers' perspective is the extremely low distribution cost, which includes the transaction costs of payment. DRM solutions that reduce the cost of providing (and restricting) access from the need to transfer and store the whole content in a secure fashion to transferring and storing rights objects securely, which is orders of magnitude cheaper. Without DRM, these costs would be clearly prohibitive for high-quality video content, while introducing DRM would make it applicable to practically any kind of digital content ranging from poetry and simple still images to multiple hours of high-fidelity video (e.g. films). It is equally important for instantaneous payments to be possible and cheap. In the case of payments, even intangible costs like the effort and time required to make the payment become significant. This is one of the greatest challenges in making such a system feasible.

Bottom line

We have outlined two content distribution models, which do not depend on copyright and use DRM solutions to lower transaction costs while keeping transactions secure. Unlike the case of copyright enforcement, the proposed business models do not provide manufacturers and users of DRM-enabled devices (that is, those in the very best position to defeat DRM solutions) with incentives to actually sabotage and attack DRM.

They do, however, provide sufficient incentives to author and share creative content, which has historically been the role of copyright. While copyright was perfectly adequate in a world where transaction costs and copying costs were reasonably high, it is becoming increasingly controversial and difficult to enforce in a networked, digital world. In particular, DRM techniques regularly fail as copyright enforcement tools, primarily because of misaligned incentives. In the proposed business model, for which copyright is not relevant, DRM is a tool of lowering transaction costs together with a peer-to-peer digital currency.

Sources

- Boldrin, M. and Levine, D. K. (2005): Intellectual property and the efficient allocation of social surplus from creation. Review of Economic Research on Copyright Issues, 2005, vol. 2(1), pp. 45-66; http://levine.sscnet.ucla.edu/papers/rerci_revised.pdf
- Cullen, J. (2005): Music industry fails to stamp out digital piracy. BBC6 Today's Music News, Dec 5, 2005; http://www.bbc.co.uk/6music/news/20051220_download.shtml
- Dufft, N. (2005): Digital music usage and DRM. Results from a European consumer survey. INDICARE; http://www.indicare.org/survey

- Fortunato, S. et al. (2005): The egalitarian effect of search engines. arXiv.org, Nov 1, 2005; http://arxiv.org/abs/cs.CY/0511005
- Mackenzie, D. (2005): Soft cash in, hard cash out. New Scientist, 2005, issue 2509, pp. 40-43; http://www.newscientist.com/channel/info-tech/mg18725091.800.html
- Madden, M. (2004): Artists, musicians and the internet (survey findings). Pew Internet & American Life Project; http://www.pewinternet.org/pdfs/PIP_Artists.Musicians_Report.pdf
- Nagy, D. A. (2005): On cash-like digital payment systems, International Conference on Electronic Commerce and Telecommunication Networks, Reading, UK, Oct 3-7, 2005; http://www.epointsystem.org/~nagydani/ICETE2005.pdf
- Orlowsky, A. (2004): iTunes DRM cracked wide open for GNU/Linux. The Register, Jan 5, 2004; http://www.theregister.co.uk/2004/01/05/itunes_drm_cracked_wide_open/
- Rubens, P. (2002): Border controls crumble in DVD land. BBC NEWS dot.life, Aug 19, 2002; http://news.bbc.co.uk/1/hi/in_depth/sci_tech/2000/dot_life/2197548.stm

About the author: *Daniel A. Nagy* is an information security expert, interested in financial cryptography and the economics of cyberspace. Currently, he works for SEARCH-LAB Ltd, Budapest. He is also the lead developer of ePointSystem.ORG.

Status: first posted 15/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=172

The Future Digital Economy: A session report on DRM

By: Philipp Bohn, Berlecon Research, Berlin, Germany

Abstract: On January 30th and 31st, the Organisation for Economic Co-Operation and Development (OECD) and the Italian Minister of Innovation and Technology, *Lucio Stanca*, invited delegates from all OECD countries to Rome. Several speakers were scheduled to discuss digital content creation, distribution and access. One panel specifically addressed "Content diffusion: IPR, DRM, licensing, content security, standards". This article summarizes some key ideas and statements, primarily concerning DRM.

Keywords: conference report – business models, digital media, interoperability, intellectual property, standards

Introduction

During the conference a wide range of success factors for the digital economy was discussed: availability of broadband access was stressed as a crucial prerequisite for most business models, the importance of amateurization – enabled by cheap ways to produce and alter digital content and make it available through the Internet – was introduced by *William Fisher* (Director, Berkman Center of Intellectual Property Law) in his dinner speech and was picked up by several speakers later on. Convergence of media and services was another trend identified, threatening established players and giving opportunities to new market entrants that profit from low barriers to entry – think e.g. of Voice over IP. Public sector information was another important topic opening new business perspective. The BBC for example is starting to make older documentaries and movies available to the public via the Internet.

There is apparently no easy answer to the role of governments and their agencies confronted with these rapid developments. One fundamental policy issue however coming up again and again across panels and plenary sessions was the need for a fair balance in intellectual property rights including DRM. For instance *Toyoda Masakazu* (Director-General, Japanese Ministry of Economy, Trade and Industry) called for an unbundling of the operating and DRM systems to prevent the emergence of monopolies (Apple and Microsoft are trying to strengthen their market position using their respective DRM sys-

tems). *Rita Hayes* (Deputy Director General, Copyright and Related Rights and Industrial Relations, WIPO) suggested a common approach to DRM standards, especially regarding device- and content-interoperability. *Michael Geist* (Professor, Canada Research Chair in Internet and E-commerce Law, University of Ottawa), suggested that content companies from the movie and music industries should reduce their reliance on DRM – a practice that "locks down" content (cf. Geist 2006).

In the following this report will concentrate on the panel dedicated to DRM and related issues. The mere fact that a special session on these issues took place is another indicator of the importance of IPR and DRM for the future of the digital economy.

Panel discussion on DRM

The following persons were asked to join the panel (in order of appearance): *Marco Ricolfi* (Professor, University of Turin, Law School) as the panel's chair, Stan Liebowitz (Professor, Center for Analysis of Property Rights and Innovation, University of Texas), Leonardo Chiariglione (CEO and Digital Media Strategist, CEDEO.net), Fred von Lohmann (Senior Intellectual Property Attorney, Electronic Frontier Foundation), Giorgio Assuma (President, Italian Collecting Society SIAE), Barney Wragg (Senior Vice President eLabs, Universal Music Group International) and Sarah Deutsch (Vice President and Associate General Counsel, Verizon Communications).

Marco Ricolfi introduced the topic by pointing out the long and the short route of content distribution. Traditionally, there has been a large number of intermediaries between producers and consumers. While intellectual property rights as well as technological infrastructure is tailored to the long route, with digital distribution there might also be shorter decentralized routes between producer and consumer. As chairman of this session Ricolfi put in further interesting arguments in the course of this afternoon. He picked up e.g. the phenomenon of amateurization and called for the new IPR rules to be compatible with this type of content. Touching on the debate on the copyright term, he considers it to be too extensive, often hindering innovation (e.g. in case of software development). A further question worth considering was in his view, whether DRM-based solutions will alter the role of collecting societies that traditionally represent artists' rights.

Stan Liebowitz's introductory presentation focused on "Promises and Threats of the Digital Economy". Digital distribution is a very efficient way of distribution, which continues to have a significant impact on the music industry. However, consumers are adapting only hesitatingly to commercial channels: While in 2003 2% of the record industry's revenue was derived from online sales, this figure was still only 5% in 2005. Liebowitz specifically blamed rampant P2P use for the slow uptake of commercial offerings and called for further support from the side of governments.

Leonardo Chiariglione lamented about the "miserable state of debate" concerning digital media and rights management. He made an important distinction between "enforcement" and "management" of digital rights. While DRM by nomenclature should be rights management, it is in most cases the enforcement of rights. As such, it reduces economies of scale, and is often difficult to manage due to its proprietary nature. Although a "DRM conversion box" for incompatible DRM systems might offer some relief, no such technology has been embraced in a significant way. Also, proprietary DRM systems' lack of interoperability lowers the profitability of the whole digital value chain. In his view, only an open DRM standard as put forward by the Digital Media Project (DMP) offers a viable alternative. Part of "Plan B", what Chiariglione called a "liberating message", is the idea that each stakeholder in the market can decide individually on the level of protection.

Fred von Lohmann warned that using the terms "consumers" and "customers" or even "stakeholders" is framing the discussion about usage rights and protective measures in a way that is not desirable. The discussion should rather be about what "fans" or "the public" want. It is accepted for various other online services that success comes with the

ability to deliver a "cool user experience". However, this appears to be a minority opinion when it comes to digital content distribution. In particular, incompatible DRM systems limit content usability and accessibility.

But there is also great opportunity in digital content distribution, such as sharing content and experiencing community. This was possible only to a very limited degree with physical media such as CDs, which von Lohmann referred to as "frozen cultural artifacts".

Being a copyright lawyer by training, he stressed that innovative technologies like cable TV or VCR could only be developed and introduced to the market due to gaps in intellectual copyright law, not thanks to tight legislation. He proposed that intellectual property law should be interpreted generously during the early developmental stages of the digital economy. New legal regulations should be formulated ex-post, reflecting the actual evolution and the proven need of regulation. That's what he proposed as his "Plan B".

To get an idea of what consumers expect to do with content, decision and policy makers are well advised to go to places where people "don't know any better" and "innovate anyway", such as the blogosphere and other amateur sites. This could give guidelines as to how laws should be drafted or technology and business models be developed.

Giorgio Assuma maintained that also in the age of digital distribution, artists need to rely on collecting societies. Without them, it would be impossible to efficiently manage and protect digital rights. He pointed out that this could be done in a more transparent way, due to technological developments.

As a representative of a major record label, *Barney Wragg* expressed some annoyance about constant accusations from certain stakeholders in the digital economy. Rather than hindering market developments, record labels are actively promoting them with new business models – for example made-for-mobile content, portable subscriptions, licensed P2P networks as well as on-demand services based on advertising revenue. Virtually every major label has built up its own digital label, releasing songs via the Internet rather than on CDs.

According to Wragg, his label has two main objectives: One was to offer many profitable services, the other was the protection of artists' intellectual rights. Limiting factors for the success of digital distribution are lack of DRM interoperability as well as inflated financial expectations from participants along the value chain, especially on the side of mobile operators.

Sarah Deutsch praised the importance of the Digital Millennium Copyright Act (DMCA) and the WIPO (World Intellectual Property Organization) treaties for digital content production and distribution.

With communication providers trying to move up the value chain, content is of utmost importance for Verizon. The company's on-demand video offering, FiOS, delivers content encrypted end-to-end, in order to curb infringement.

When infringement is detected within Verizon's network, the company sends a warning note to the offending user. Content providers (e.g. Disney) are not notified about this act, as a measure to safeguard customers' privacy. Only in case of continued violation of copyright law the user faces contract termination.

However, it is only a matter of time until consumers "wake up" to the limits of DRM. This means that all companies on the digital economy's supply side have a considerable responsibility to balance user interests and the protection of intellectual property.

For example, customers might experience frustrations caused by DRM when they migrate to a new mobile phone. Verizon made the effort to educate its customers that no songs would be lost if they backup their licenses. Deutsch called for standardization of DRM systems and expressed the hope that non-interoperable DRM systems might one day be referred to "that recent unpleasantness".

Bottom line

The Conference helped to address frictions, discuss possible solutions and also prepare for future developments of a dynamic digital economy. Attitudes towards DRM as an efficient means to protect digital content vary significantly. While major content providers tend to stress the importance of deploying such technical protection measures, smaller stakeholders and activist groups point out risks and obvious challenges. It would have been interesting to also hear a representative from one of the major consumer electronics manufacturers or technology providers, such as Apple, Sony and Microsoft, who are often blamed for not engaging in the deployment of interoperable DRM standards.

Sources

- Conference website with more information on the conference, presentations and webcasts: http://www.oecd.org/sti/digitalcontent/conference
- Geist, Michael (2006): Locking down our digital future. BBC news, 8 February 2006; http://news.bbc.co.uk/1/hi/technology/4690188.stm

About the author: After having graduated from University of Mannheim (Business Administration), *Philipp Bohn* joined Berlecon Research as Junior Analyst in 2005. He is a member of the INIDICARE-team. Contact: pb@berlecon.de

Status: first posted 20/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=173

Research into user-(un)friendly DRM. A review

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The study *privacy4DRM* reviewed here offers on the one hand a noteworthy contribution to conformance testing of DRM systems with respect to privacy, and on the other hand a harsh criticism of traditional business models relying on DRM systems combining copy protection and personalisation of content. Perspectives of new consumer-oriented business models combined with user-friendlier technical solutions are sketched.

Keywords: review – business models, consumer expectations, data protection, DRMS, music markets, privacy, technology assessment

Introduction

The German Ministry for Education and Research (BMBF) established a line of research funding called "Innovation and technology analysis" (ITA). The publication reviewed here is the outcome of such a sponsored project on DRM (cf. ITA-BMBF). Project partners were the Fraunhofer Institute for Digital Media Technology (IDMT), a data protection agency (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein), and a university (Technical University Ilmenau). The title *privacy4DRM* tells about the *main* focus of the project: to investigate privacy with respect to existing e-commerce platforms relying on DRM systems. The cases analysed are:

- Apple's iTunes (Fairplay),
- T-Online's Musicload (Windows Media Rights Manager - WMRM),
- Sony's Connect-Europe (OpenMG),
- Bevision-Shops (based on the PotatoSystem), and
- Adobe's Digital Media Store (PDF).

In addition to the techno-legal privacy analysis performed, the study also attempts to provide a broader explanation why the dominant business model in online music markets based on strong DRM does not work.

In the following the review will present first the structure of the study, second the main findings of the privacy analysis, and third the main arguments of the more general reasoning. Finally we will discuss the findings. As the study (Bizer et al. 2005) is in German, I will also draw on two related articles in English (published in the Axmedis proceedings: Grimm 2005, and Will 2005). A short article by Bizer et al. (2006), which resumes the study in 6 pages, has also been considered for this review.

Overview of the study

Chapter 1, the introduction, explains the objective of the study: to come up with a catalogue of criteria for user-friendly and privacy-conforming DRMS, to be applicable not only to the music market, but also to other markets like the educational market. In the introduction you also find an outline of the legal framework of privacy and copyright.

Chapter 2 on "methodology" sets out the legal, economic and technical criteria to be applied, and sketches how the interdisciplinary analysis was performed. On the one hand data flows and traces were tracked down and checked if they conform with the criteria of privacy. On the other hand the economic analysis of the download platforms addressed the value propositions for consumers, the revenue and business models of the content providers, and transaction costs from both points of view, the consumers' and the businesses'.

Chapter three to seven describe the 5 services chosen (see above) and present the findings of the different analyses one by one. Chapter 8 gives an overview of these findings.

Chapter 9 called "mission" contains what might be better termed "conclusions", as the findings are discussed here at a general level addressing policy issues, and proposing more consumer orientation and more user-oriented DRM systems design.

The last chapter is titled "recommendations for action". The first part of this chapter discusses if and how the results derived from the music market can be applied to the areas of education, learning, and research. While the same rules may apply for e-learning materials such as books, music, and video, interactive learning tools clearly need different types of access and usage control comparable to those for computer games and interactive software (Bizer et al. 2005, p. 204f).

The second part of chapter 10 comes up with six topics deserving further research: (1) new distribution models and new services are still lacking appropriate protocols and infrastructure concepts; (2) new distribution models for digital libraries, educational publishing, and research publications are particularly challenging in this respect; (3) economic research on incentive models for new distribution models is needed; (4) comprehensive risk management of DRM-systems is still lacking; (5) it is still an open question how to implement pseudonymity concepts in DRM systems and how to legally frame them, and finally (6) the idea of "privacy labels" (Datenschutzgütesiegel) is put forward.

DRM and privacy

The most innovative aspect of the study is in my view its scrutiny of data flows taking place and data traces being produced when using DRM systems. In order to analyze DRM systems, the authors use a privacy model which is in line with the European data protection directive (EU 1995; Grimm 2005, p.108) and also conforms with corresponding national regulations. The result of this analysis is that state-of-the-art DRM systems "collect more personal data from their customers than necessary to fulfil the purchase service. There are many hidden interfaces, both by encoding personal data within the products, and by linking clickstream data with contractual data" (Grimm 2005, p. 112).

Even if knowledge about customers may be used exclusively to improve the service, the fact that e-content providers hide their actions to consumers, shows a lack of trust, which in turn leads to a lack of trust on the consumers' side when they become aware of this. A particularly disturbing finding is the encoding of personal data within digital products. This action is again intransparent to the customers. In other words, forensic DRM, meant to trace illegal behaviour, is

added to the DRM system. As the authors put it: "… most shop systems which use DRM, do not trust the built-in mechanisms of DRM to enforce the usage rules in the end-user devices. Therefore they use the trace method as a second line of defense. They collect data to identify users, not only for business purposes, but also to link products to their buyers in order to identify the origin of products in illegal environments." (Grimm 2005, p. 108; Bizer et al. 2005, p. 198). The good news if you like: there was no proof that the investigated systems collect data about individual usage patterns. If this were the case it would clearly violate existing privacy legislation (Bizer et al. 2005, pp. 183, 192).

A pro-active, transparent policy by the content providers involving the consumers could alleviate the situation to a certain extent. The situation could be further improved by implementing pseudonymity options, as many marketing purposes don't require information about the persons using a service (Bizer et al. 2005, p. 200). A third measure proposed to increase trust are "privacy labels" guaranteeing that the DRMS is respecting privacy. This approach might be highly interesting for those in favour of conformance testing like the Transatlantic Consumer Dialog (cf. their DRM declaration with respect to privacy; TACD 2005).

Assessing "state-of-the-art" DRM systems

As stated above the study also aims to assess what they call "state-of-the-art" DRM systems in the context of music markets. I will try to boil down their reasoning to 10 points.

1. No doubt, a balance is needed between the right of creators to obtain remuneration for their creative work, and the interests of end-users and the public.

2. In the currently dominating business model content is to be sold analogue to physical goods, i.e. as a digital object. DRM is meant to enable the old business model by protecting the digital object.

3. In order to achieve this, "classical" DRM couples content, client, and device (Bizer et al. 2005, p. 181). To get access to purchased content, the end-user now has to legitimize himself or herself to the digital object. Furthermore DRM systems add data collection to copy protection. On top, as a second line of defense, forensic DRM using personal data is added to strong copy protection (p. 188, 191). As an important aside the authors argue, that assuming personalisation of content (forensic DRM) is already a matter of fact, the request of content providers to get a right to get personal information from the ISP appears excessive and unnecessary (p. 182).

4. The way DRM systems are designed and implemented is contrary to a basic principle of IT-security, namely that the party interested in the protection must have the means to enforce the protection. This is difficult in the case of DRM systems, because the mechanisms to enforce the protection are located on the end-user's side. Ultimately he or she is sovereign of the computing device (p. 17). Cooperation can not be expected and circumvention is a reality – in particular if the value proposition for end-users is poor.

5. The lack of acceptability of protected content is due to at least three shortcomings of current DRM systems:

- (1) immature technology excluding even uses foreseen by the providers (e.g. playing a CD at home and in the car; p 197f),
- (2) DRM systems not respecting either fair use or allowing for the copyright exceptions granted by law (p.197), and
- (3) non-interoperable technology putting the burden on the consumers having to implement and purchase multiple tools and devices to get what they want (p. 197).

6. The lack of acceptability of protected content is due also to a defective trust relationship between business and consumers. Forensic DRM, when performed in an intransparent way, and anti-piracy campaigns criminalizing customers undermine trust.

7. The authors assert that existing music download platforms using DRM-systems are in reality not a success (p. 193-195) – not even iTunes.

8. Consumers are supposed to decide whether to purchase legal content on the basis of an transaction cost calculus. "The customer is willing to pay for the avoidance of expected transaction costs when downloading illegally. He is not willing to pay for the usage of the data" (Will 2005, p. 99).

9. Within the current paradigm the situation can be improved, if DRM systems are designed conforming to privacy principles, with increased end-user involvement, more user-friendly design, and with greater interoperability.

10. However this cure might not be enough and alternative business models and revenue models need to be developed, focussing on services. People would be willing to pay for added value (recommendations, preview etc.). Users might also accept collection of personal data if they get in turn more individualised services. Content providers should actively involve end-users providing them with more options and choice what usage rights to obtain. Under these conditions, new services based on "user-oriented DRM" (p. 199) are more likely to be accepted.

Discussion

While old DRM seems to be the illness it purports to cure (adapted from *Karl Krauss*, the Austrian writer's famous sentence about psychoanalysis), new user-oriented DRM seems the healthy way out. By and large I share the reasoning presented, and indeed INDICARE has always pointed to the shortcomings of the old business model and the potential of new business models (cf. e.g. INDICARE 2004). However I would like to add six remarks to enrich the picture drawn by the authors.

1. With respect to transparency and user involvement requested, when it comes to data collection and privacy, I would go even further and stress the potential of combining DRM and PET (privacy enhancing technology) as Korba and Kenny (2002) have done in their seminal paper "Towards meeting the privacy challenge: Adapting DRM" (cf. also Tóth's introduction to Privacy Rights Management (PRM) in the INDICARE Monitor 2004).

2. I would not underline that legal download platforms can't be a commercial success. Although the IFPI:06 Digital Media Report's message "legal online buying is catching up with illegal file-sharing" contains a considerable portion of wishful thinking, the strategy of the music industry combining law suits against P2P file sharing services, legal actions against individual uploaders (ca. 20.000 in 2005, cf. IFPI 2006, p. 18), threatening campaigns, deteriorating quality of content on filesharing servers, and improving their own offerings in terms of scope and interoperability should not be underestimated. There is no *a priori* that the big players of the music industry *must* fail.

3. I can imagine new service oriented offerings ruled by somehow transparent DRM. I can also see that these might be perceived as a "fair deal", thus increasing the acceptance of those services. But would this change the basic flaw of DRM as pointed out by the authors themselves, namely that DRM systems are not in line IT-security principles (see point 4 above)?

4. While I see the potential of new business strategies where you pay for added-value and not for content, I doubt if this model does justice to creators, and I am afraid that this approach might also help to erode the foundations of copyright and creative works.

5. An important reason why consumers behave illegally and why people feel so uncomfortable with DRM is not mentioned. Restrictions imposed by DRM violate the consumers' sense of ownership. The intuitive understanding of "property" is linked to ideas such as long term possession, unlimited use and the right to resell. Remember Thomas "If men define situations as real, they are real in their consequences" (the so called Thomas theorem). The fact that property rights with respect to digital goods imply a change from ownership to rights of disposal (licensing) is obscured even by the content industries themselves - still suggesting that you buy music when you pay for it. This argument has been elaborated in an INDICARE Moni-

tor article about the mind-set of pirates (Böhle 2005).

6. The authors introduce type of *homo oeconomicus* who calculates transaction costs when looking for content (see point 8 above). This argument has to be differentiated based on the previous remark, and furthermore because empirical research tells us that consumers are willing to pay for content itself if the payment (or a considerable share of it) goes to the creators themselves (cf. Madden 2004; see also Regner and Barria 2005). Consumer behaviour is obviously more value-oriented than expected. You may play the David-Goliath-game, while at the same time respecting creators. Research into piracy (see point above) also indicates that the social reputation to be gained from savvy filesharing within groups is rather important.

Bottom line

The most innovative aspect of the study is in my view its scrutiny of data flows taking place and data traces being produced when using DRM systems, combined with concrete ideas on how to improve the situation: by transparency, pseudonymity options, and "privacy labels". The general reasoning on DRM has very strong points like the contradiction between DRM systems and IT-security. Consumer behaviour, however, seems to be modelled in a too abstract fashion disregarding social factors.

Sources

- Bizer, Johann; Grimm, Rüdiger; Will, Andreas (2006): Privacy4DRM: Nutzer- und datenschutzfreundliches Digital Rights Management. DuD • Datenschutz und Datensicherheit ,30 (2006) H 2, pp. 69-73
- Bizer, Johann; Grimm, Rüdiger; Möller, Jan; Müller, Michael; Müller, Anja; Jazdzejewski, Stefan; Puchta, Stefan; Will, Andreas (2005): Privacy4DRM, Datenschutzverträgliches und nutzungsfreundliches, Digital Rights Management, Kiel/Ilmenau; http://www.datenschutzzentrum.de/drm/privacy4drm.pdf
- Böhle, Knud (2005): About the mind-set of software pirates. INDICARE Monitor; Vol. 1, Number 8, January 2005; http://www.indicare.org/tiki-read_article.php?articleId=74
- EU (1995): Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; http://europa.eu.int/comm/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
- Grimm, Rüdiger (2005). Privacy for Digital Rights Management Products and their Business Cases. In: Nesi, Paolo; Ng, Kia; Delgado, Jaime (eds.) (2005): Proceedings of the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution, IEEE Computer Society, pp. 107-112
- IFPI (2006): IFPI:06 Digital Music Report; http://www.ifpi.org/site-content/library/digital-music-report-2006.pdf
- INDICARE (2004): Helberger Natali (ed.); Dufft Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich: Digital rights management and consumer acceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report, Amsterdam, December 2004; http://www.indicare.org/soareport
- ITA-BMBF: http://www.innovationsanalysen.de/de/projekte/digital_rights.html
- Korba, Larry and Kenny, Steve (2002): Towards Meeting the Privacy Challenge: Adapting DRM. NRC paper number NRC 44956, November 2002, http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-44956.pdf
- Madden, M. (2004): Artists, musicians and the internet (survey findings). Pew Internet & American Life Project; http://www.pewinternet.org/pdfs/PIP_Artists.Musicians_Report.pdf
- Regner, Tobias and Barria, Javier (2005): Magnatune – A voluntary-based model for online music. INDICARE Monitor, Vol. 2, Number 8, October 2005; http://www.indicare.org/tiki-read_article.php?articleId=147
- TACD (Transatlantic Consumer Dialogue) (2005): Resolution on Digital Rights Management http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=275; or http://www.tacd.org/db_files/files/files-380-filetag.doc
- Tódt, Gergely (2004) DRM and privacy - friends or foes? An introduction to Privacy Rights Management (PRM). INDICARE Monitor; Vol. 1, Number 4, September 2004; ;http://www.indicare.org/tiki-read_article.php?articleId=45

► Will, Andreas (2005): An economic analysis of music download platforms: Proceedings of the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution, IEEE Computer Society, pp. 97-100

About the author: *Knud Böhle* is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 22/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=174

Informed consumers should welcome the implementation of *effective* DRM – if it meets their needs

By: Mark Bide, Senior Consultant, Rightscom Limited, London, United Kingdom

Abstract: The need to protect intellectual property is part of a much wider – and increasingly urgent need – to implement a wider framework of "digital policy management" on the network. Consumers will not only accept digital policy management but will welcome it – so long as it is designed to meet their requirements and expectations, not simply to defend the existing business models of today's media and technology businesses.

Keywords: opinion – consumer, copyright exceptions, policy management, DRMS, e-commerce, trusted computing

Introduction

We must seek out a new approach to managing trust on the network.

To date, our halting attempts at cobbling together a "digital rights management" solution have been at best unconvincing, at worst completely inept – because they have been exclusively focused on protection of intellectual property rights, and have approached the issue in a very limited way. What we now call "DRM" needs to evolve into something which perhaps we will come to call "Digital Policy Management" – a new technical approach to managing trust on the network.

Some of the policies we want to manage in this way may indeed be rooted in intellectual property rights protection. But others will stem from personal or corporate policies (like privacy and confidentiality); yet others may come from interpretation of the legal code. Effective protection of intellectual property – in a manner that is acceptable to consumers – should be a side effect of this new "Digital Policy Management" approach to managing trust, not the main event.

Building a framework for network citizenship

The challenge of maintaining a framework for protection of intellectual property on the network is closely related to many other challenges which are facing us on the network. Despite the best efforts of both lawmakers and of those who would enforce the law, users bent on using the internet with felonious intent persistently stay one step ahead. Fraud is rife, and fraudulent emails become ever more sophisticated. Attempted extortion based on denial of service attacks has recently been exemplified by the attack on "Million Dollar Homepage" (cf. Gonsalves 2006). Although the recent attack of the Kama Sutra virus may not have been as disastrous as predicted (BBC 2006), viruses and spyware continue to proliferate throughout the network. And spam, while perhaps exemplary of a rather different level of malfeasance, creates a problem for every user of

the network that is – in its totality – immensely costly.

At first sight, these "network citizenship" issues may appear to have little link with intellectual property and digital rights management, but the problem in all these cases is one of trust and trusted identity.

Our response to the attack on trust on the network has been somewhat feeble. Trust circles, like those based on "friend of a friend" (cf. sources) linking of personal web pages – or more business oriented approaches like LinkedIn (cf. sources) – undoubtedly have a role to play; but they don't deal with the problem of the outside world, with the fact the Internet is (as I have recently seen it described; Becker 2006) a "world of strangers" – nor with the reality that those strangers are not universally benign. To move beyond this world of strangers, we need to move from concepts like trust circles to more robust mechanisms that allow us to truly trust one another's assertion of identity and to grant appropriate permissions to those that we do trust.

Renewing trust on the Internet

In a recent article (Talbot 2005), *David Clark* of MIT, an Internet pioneer, is quoted as saying: "We might just be at the point where the utility of the Internet stalls – and perhaps turns downward" – because of the growing loss of trust. The economic and social implications of a widespread loss of trust in the network are incalculable; it is now integrated into our lives at a very deep level.

In a similar vein, *Vint Cerf,* one of the "founding fathers" of the Internet, and now Google's "chief internet evangelist" was recently quoted (Talbot 2006) as saying: "I believe the potential growth of the Internet will be limited if we allow invasive badware and spyware to continue to fester without strong action. All consumers must be in control of their experiences when they browse the Internet and the mass proliferation of badware threatens this control. We cannot allow that to continue…. The providers of Internet services and software simply must get this problem under control."

You do not necessarily need to share the view that we urgently need a complete re-engineering of the fundamental architecture of the Internet to recognise that there is real enough problem to address. Nor is it necessary to accept uncritically the architecture proposed by the Trusted Computing Group (TCG; cf. sources), which appears to run the risk of putting an excessive amount of power into the hands of a small number of technology companies. In the circumstance, the words "trust", "trusted" and "trustworthy" can all become a little slippery.

No one will easily be brought to trust technology solutions which threaten "lock in" to particular providers of technology, and to hand power to a technocracy.

Avoidance of lock in is dependent on interoperability and low switching costs, something that the TCG proposals could impose considerable limitations on. Interoperability is therefore the key challenge – and interoperability will depend on the availability "policy metadata": clear, unambiguous and standardised ways of *expressing* policies – in many ways, building this layer of policy data is a much more significant task than *enforcing* the policies.

Indeed, the ability to express the policies in a standard, interoperable way provides us individually with options – options as to whether policies are to be enforced through technology (in the context of intellectual property, think "DRM") or through a combination of trust, good will and the law (think "Creative Commons").

Of course, there is potential downside to the interpretation of essentially *uncertain* legal concepts into the *certainty* of machine-interpretable code. It becomes necessary to hard code concepts of "reasonableness" and "proportionality", things that are by their nature contextual. This inevitably creates a challenge in areas like exceptions to copyright; but we should face up to those challenges rather than simply spike them as "too difficult".

Maintaining the balance

We do well to remember that copyright was established for the good of society: "To pro-

mote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries" (US Constitution). Technology should no more be used to extend the intended scope of copyright protection than it should be used to destroy its central purpose.

There can be few who still doubt that the internet will prove to be a hugely disruptive technology for the copyright industries, just as it proving hugely disruptive for other sectors. However, before deciding that we want to dispose of the entire structure of intellectual property, we should be sure that we have fully considered the consequences.

Ultimately, effective management and protection of intellectual property on the network will only be possible within a framework of trusted (and trustworthy) network computing. However, the primary motivation for the implementation of such a framework will not be the protection of the current business models of the media and technology industries (who have not always acted in ways guaranteed to make themselves popular with consumers).

Consumers will welcome the introduction of digital policy management technology – including management of "digital rights" – only if it also offers a solution to *their* underlying security and identity problems and contributes to the maintenance of civil society on the network, with all the complex checks and balances that this implies. This will not easily be achieved, but that does not mean that it is not worth the effort.

Sources

- BBC news (2006): "Limited" damage from Nyxem virus. BBC News 3 February 2006; http://news.bbc.co.uk/1/hi/technology/4677022.stm
- Becker P. (2006): A world of strangers" The Digital ID World Newsletter 2 February 2006; http://www.digitalidworld.com/modules.php?op=modload&name=News&file=article&sid=318
- Gonsalves, A. (2006): "Million Dollar Homepage" targeted in huge denial-of-service attack. Information Week 13 January 2006; http://www.informationweek.com/news/showArticle.jhtml?articleID=177100372
- LinkedIn: https://www.linkedin.com/
- Talbot, D. (2005): The Internet is broken" Technology Review 19 December 2005; http://www.technologyreview.com/InfoTech-Networks/wtr_16051,258,p1.html
- Talbot, D. (2006): Google, Sun Backing New Anti-Malware Effort" Technology Review 25 January 2006; http://www.technologyreview.com/InfoTech-Software/wtr_16184,300,p1.html?PM=GO
- The Friend of a Friend Project: http://www.foaf-project.org/
- Trusted Computing Group: https://www.trustedcomputinggroup.org/home
- US Constitution, Article 1, Section 8: http://www.archives.gov/national-archives-experience/charters/constitution_transcript.html

About the author: *Mark Bide* is a Senior Consultant at Rightscom Limited, a specialist consultancy based in London which was founded in 2000 to support the design and deployment of business, technology and process solutions in the management, protection and trading of intellectual property rights and content in the digital environment. Mark has over 30 years experience in the publishing industry, having been a Director of the European subsidiaries of both CBS Publishing and John Wiley & Sons. With a background in production, distribution, and publishing technology, he has been a consultant for nearly 15 years and has particular expertise in the impact of network technology on the information value chain. He has been closely involved in standardisation strategies to support the management of intellectual property on the network. Contact: mark.bide@rightscom.com

Status: first posted 22/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=175

Trusted computing for digital rights management

By: Robert A. Gehring, Computers and Society, Technical University, Berlin, Germany

Abstract: The relationship between trusted computing (TC) systems and digital rights management (DRM) systems is discussed. Trusted systems technology was developed in the 1960s, while the modern concept of DRM is a brainchild of the Internet era of the 1990s. While TC technology can be used to build DRM systems, both belong to different categories and should not be confused. TC technology may as well be deployed to protect "darknets" (Biddle et al. 2003) for sharing data. Making TC-based "copyright boxes" (Stefik 1999) is by no means a guarantee for business success in marketing digital content where consumer demand is ignored.

Keywords: technical analysis – consumer expectations, file sharing, DRMS, trusted computing

Introduction

First things first. No, trusted computing (TC) is not the same as digital rights management (DRM). DRM technology has been built, and will be built in the future, entirely without relying on TC support. And yes, DRM can be based on TC technology, as Chinese PC maker Lenovo has just demonstrated (cf. Dornan 2006).

According to Information Week, Lenovo's latest ThinkPad model uses a fingerprint sensor in combination with a trusted platform module chip (TPM) and software support from Microsoft and Adobe for controlling access to, and distribution of, PDF documents (Dornan 2006). Lenovo's DRM approach ties biometrics, content (i.e., documents), and TPM support, in order to enforce usage rights and monitor actual use of the content. Accessing a "controlled" PDF document first requires authentication through fingerprint identification; without authentication, access is denied. The creator of the document is the one who determines who subsequently may access the PDF. The Lenovo system is also prepared to track acts of accessing and reading the document, and reporting this information. Whether the TPM plays a key role in the scenario is unclear as of now.

Depending on your standpoint, Lenovo's innovation may be "particularly frightening" (Dornan 2006) or a good thing. And that exemplifies the crux of trusted computing in general: What is good use or evil use depends on purpose and positioning. In itself, trusted computing is merely a tool, as recently pointed out by Linux kernel developer *Alan Cox*: "There's a lot of political debate, that it's really evil or good. But it's only a tool" (Marson 2006). Those who use this tool with intention will decide on its meaning.

Although TC technology has primarily been propagated for security improvement of networked end systems, multiple observers were quick to point out that some of its basic features were similar to mechanisms that allow supporting DRM. In some extreme cases, TC has literally been equated with DRM; this is, as a thinly veiled attempt to introduce ubiquitous control mechanisms on formerly open PC architectures.

As a tool for making the behaviour of computer systems more predictable, by enforcing rules on users and processes (i.e., mandatory access control), trusted computing creates ample opportunity for ruling out undesirable effects of software – and software users. At the same time it empowers parties controlling access to the rule-making process to forcing users to comply with their private interests, and to cut out competitors, when attempting to access, and use, system resources. Whether any such attempt will be successful in the long run is contingent on economical and political factors as well.

As the latest Sony-BMG debacle with the XCP and MediaMax copy protection software has shown, misjudgements of consumer expectations can easily lead to costly backlashes, and even to legal and legislative action (Helberger 2006; Leyden 2006; and see

the documentation at Groklaw 2006). Hence, the price of using digital rights management - be it based on trusted computing technology or not - may be higher than the price of foregoing access control in the first place. And as *David Pakman*, CEO of eMusic.com, emphasised, the logic of DRM is not necessarily good business logic, too: "If it were possible to demonstrate that non-DRM'ed music encourages more sales, wouldn't it make sense for the industry to offer portions of its catalog as unrestricted MP3 files? It seems like bad business to bind every category of customer and every category of product with the same sales offering" (Pakman 2005).

While TC technology may be helpful in "hardening" DRM systems, it is in no way helpful for selling music beyond demand. And if systems are almost impossible to crack, and that it is what TC promises to do, governments are highly concerned (Stone-Lee 2006). And from a content-owners point of view, trusted systems built on TC technology, in fact may well turn out as a nightmare. A network of trusted systems could be used to establish a technically impenetrable file sharing community, a TC-protected darknet (for darknets see Biddle et al. 2003).

So when discussing the relationship between DRM and trusted computing, one has to keep in mind that not everything that is technologically feasible is economically viable or politically acceptable at the same time.

This article discusses in short the relationship between DRM and trusted computing, and what makes TC technology useful for implementing DRM. For practical reasons, it is not possible here to delve into details of TC technology. Instead, the interested reader is referred to (Pearson et al. 2003; Smith 2005).

"Trusted computing is DRM": Dispelling a myth

Learning some facts about the history of trusted computing and DRM might be helpful in distinguishing the relative merits of either concept.

Historically, trusted computing has its roots in the concept of trusted systems (Kuhlmann and Gehring 2003). Trusted systems are neither new nor invented by the Trusted Computing Group (TCG), the body behind the most important TC architecture. Actually, research on trusted systems dates back to the 1960s. Efforts were driven by government and military needs for effective protection of information in the cold war era. Two research approaches proved particularly influential:

- The reference monitor (RM) concept introduced in 1973 by *James Anderson* (Anderson 2001, p.140); and
- The Bell–LaPadula (BLP) model as introduced in the same year by *D. Elliott Bell* and *Leonard J. LaPadula* (Anderson, Stajano and Lee 2001, p.189).

While Anderson's reference monitor has been conceived as a proposal for governmental establishments, BLP was developed for a military environment with well-defined security requirements.

BLP was primarily designed to deal with restricting the information flow between formally distinguished security levels and compartments. The RM concept, on the other hand, models a system architecture suitable to enforce arbitrary access control policies. It can be regarded as a container to be filled with a rule set of choice. As such it is pretty generic and flexible - "an abstract machine that mediates all accesses to objects by subjects" (Bishop 2003, p.502).

Once filled with an access control policy, i.e. specific rules for access control, a reference monitor will enforce that policy. A validated, tamper-resistant implementation of a RM forms the policy-core of a trusted system, its so called trusted computing base (TCB), and "consists of all protection mechanisms within a computer system - including hardware, firmware, and software - that are responsible for enforcing a security policy" (Bishop 2003, p.502).

Note the interplay of "hardware, firmware, and software" making the trusted system work. One important but often overlooked property of the *trusted system concept* is its policy-neutrality; it was not designed as a DRM concept (see below). In practice, however, *concrete trusted systems* will enforce specific policies. It depends on all three fac-

tors –"hardware, firmware, and software" – which access control rules will be enforced. In other words, hardware vendor, firmware vendor, and those who provide and configure the system's software stock, will set the rules. Conceptually, trusted systems are as able to enforce DRM policies as they are to enforce "mandatory open-access" (think of a system that refuses to create files with access control attributes).

TCG (former TCPA) and trusted systems

Founded in 1999 by Compaq, HP, IBM, Intel, and Microsoft, the Trusted Platform Computing Alliance (TCPA) was relaunched in 2003 as the Trusted Computing Group (TCG). As of January 2006, the TCG had more than 120 members.

The TCG's mission is to "develop and promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms" (Trusted Computing Group 2006). It does not provide hardware or operating system software.

TCG specifications exist so far for:

- Infrastructure Specifications
- PC Client Specifications
- Trusted Platform Module (TPM) Specifications
- Trusted Network Connect (TNC) Specifications
- TPM Software Stack (TSS) Specifications
- Server Specific Specifications

The one outstanding advantage the industry-wide approach of the Trusted Computing Group has to offer for building trusted systems is that it *standardises components*. TC enables mass-production of hardware components and reuse of software components, thus making it comparatively cheap to build trusted systems.

From trusted systems to DRM

Digital rights management (DRM) is a relatively new development going back to the 1990s. *Mark Stefik*, researcher at Xerox's Palo Alto Research Center, promoted the idea of "usage rights management" (Stefik 1996a, p.221) – a term much more appropriate to describe what DRM does – for digitally distributing intellectual property. He located the root of the problem of selling content in the architecture of modern personal computer systems: "Fortunately, computers need not be blind instruments of copyright infringement. Properly designed digital systems can be more powerful and flexible instruments of trade in publications than any other medium. The seeming conflict between digital publishing and commerce is merely a consequence of the way computer systems have been designed to date." To overcome this "design flaw," he suggested using "techniques for commerce in what we call digital property rights or usage rights…several kinds of rights besides copying" (Stefik 1996a, p.221). That comes close to what DRM systems do today.

What is a DRM system?

Although, there is no single one definition for what constitutes a DRM system, the modern conception regards three elements as crucial (Rump 2003):

- Technology;
- Law; and
- Business Model.

The business model is this: keeping supply of certain binary data short and charging for metered access to this artificially "scarce resource". Technology is applied to protect this business model for marketing binary data by controlling access to, and usage of, while legal protection for technological measures discourages circumventing technological barriers to otherwise free access to data. Due to very liberal laws, there is no need for the data to represent "works of authorship" under copyright protection, and it is not hard to find an old movie, the copyright of which has expired, to be nevertheless distributed on DVD with CSS copy-protection.

The only perfect DRM system is one that can neither be broken nor avoided. And while this article focuses on the technology side, that statement refers to all three elements of DRM: If one of the three elements can be broken or avoided, the DRM system is doomed to fail.

Different approaches for implementing DRM have been broken and the content they guarded leaked onto the Internet. Thus, people had alternative ways of access to content and could avoid using DRM systems. Legal threats were no real show-stopper (IFPI 2006).

What makes TC technology especially attractive for implementing DRM is their ability to enforce usage policies. Once their security conditions are broken, TC systems stop working. Since their security conditions are built as a "chain of trust" containing hardware-locked keys and certificates from trusted third parties, they are hard to tamper with, at least much harder than software-only systems. Being able to rely on a trusted system, it is a fairly simple thing to implement a hard-to-break "usage rights management" as the platform of choice for content owners.

Coming DRM-enabled operating systems, such as Microsoft's Windows Vista flavours, are aimed at providing "casual, honest users with guidelines for using and consuming content based on the usage rights that were acquired" (*Dan Glickman*, President of the Motion Picture Association of America, in BBC 2006). That is necessary, because "[w]ithout the use of DRMs, honest consumers would have no guidelines and might eventually come to totally disregard copyright and therefore become a pirate" (ibid.). To reinforce the guidelines, trusted computing features are deployed (see the Lenovo example in the introduction), all the more appealing if components are cheap (see above).

Selling copyright boxes

Rather than modifying their age-old control-based model of making money from copyrighted works, the content industries pursued DRM as their one and only salvation from having to suffer "the fate of the buffalo" (Bronfman 2000, quoted in Fridman 2000).

The idea of using concepts developed for trusted systems as blueprints for "usage rights management" systems was widely promoted by Stefik. He argued that "the first key to commerce in digital works is to use trusted systems" (Stefik 1996a, p.228) – and apparently he was quite persuasive. Turning general-purpose computers, or special-purpose devices, into "vending machines" thus enabling potential customers "to order digital works any time of the day and get immediate delivery" (Stefik 1996a, p.228), sounded like a huge business opportunity. Transforming computers hitherto under the control of their users (often being their owners, too) into "copyright boxes" (Stefik 1999, p.55) more like radios, TV-sets, and CD-players – this idea really took off with content industries seeking to commercialise the internet after the ban on commercial activities was lifted in the middle of the 1990s.

But a DRM system is almost useless, that is from a content owner's perspective, until it is deployed broadly. Putting together cheap TC components with a market-dominating operating system "enriched" with DRM functionality is the most economic way to provide the majority of users with "copyright boxes." Microsoft is doing just that (Microsoft 2006).

Bottom line

TC technology is neither necessary nor sufficient to implement DRM but it can make implementing DRM easier and cheaper. TC components are tools – neither good nor bad. It's the way the tools are used, the interplay of "hardware, firmware, and software," that gives them meaning. And predictably, software will have the biggest part in the play, defining most of the functionality. People are using trusted systems to do things. One way to use trusted systems is to build DRM systems. But there is no way to guarantee success for DRM systems. DRM may well turn out to be "[m]edia companies' next flop" (CNET 2006) if consumer expectations are not met. And consumers want to get what, when, where, and how, they like it, without the hassle of incompatible devices. Just like in the file sharing networks.

Sources

- Anderson, R.J. (2001): Security engineering: A guide to building dependable distributed systems. New York: Wiley

- Anderson, R.J., Stajano, F., Lee, J. (2001): Security policies. In: Advances in Computers, Vol. 55, pp 185-235
- BBC (2006): Digital film: Industry answers. In: BBC Entertainment, 09 February 2006, http://news.bbc.co.uk/1/hi/entertainment/4691232.stm
- Becker, E., Buhse, W., Günnewig, D., and Rump, N., eds. (2003): Digital rights management: Technological, economic, legal and political aspects, Lecture Notes in Computer Science, Vol. 2770, Berlin, Heidelberg, New York: Springer
- Biddle, P., England, P., Peinado, M., and Willman, B. (2003): The darknet and the future of content protection. In: Becker et al. (2003), pp. 344-365
- Bishop, M. (2003): Computer security: Art and science. Boston, MA: Addison-Wesley
- Bronfman, Jr., E. (2000): Remarks as prepared for delivery by Edgar Bronfman, Jr. Real Conference 2000, San Jose, CA, May 26, 2000 (a copy of the text of the speech can be found at http://seclists.org/lists/politech/2000/May/0068.html)
- CNET 2006: DRM: Media companies' next flop? In: CNET News.com, 30 January 2006, http://news.com.com/DRM+Media+companies+next+flop/2030-1069_3-6032936.html
- Dornan, A. (2006): Yes, trusted computing is used f or DRM; Information Week, 17 February 2006, http://www.informationweek.com/blog/main/archives/2006/02/yes_trusted_com.html
- Fridman, S. (2000): Firm thinks it can solve music-pirating problem. ComputerUser.com, 31 May 2000, http://www.computeruser.com/news/00/05/31/news2.html
- Groklaw (2006): Sony DRM; http://www.groklaw.net/staticpages/index.php?page=20051122010323323
- Helberger, N. (2006): The Sony BMG rootkit scandal; INDICARE Monitor, Vol.2, Numer 9, January 2006, http://www.indicare.org/tiki-read_article.php?articleId=165
- IFPI (2006): Digital Music Report 2006. http://www.ifpi.com/site-content/library/digital-music-report-2006.pdf
- Kuhlmann, D. and Gehring, R.A. (2003): Trusted platforms, DRM, and beyond. In: Becker et al. (2003), pp 178-205
- Leyden, J. (2006): Homeland security urges DRM rootkit ban; The Register, 17 February 2006, http://www.theregister.co.uk/2006/02/17/rootkit/
- Marson, Ingrid (2006): Trusted computing comes under attack; ZDNet UK, 27 January 2006, http://news.zdnet.co.uk/internet/security/0,39020375,39249368,00.htm
- Northrup, T. (2006): Windows Vista security and data protection improvements. Microsoft, 01 June 2005, http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx
- Pearson, S., Balacheff, B, Chen, L., Plaquin, D., and Proudler, G. (2003): Trusted computing platforms: TCPA technology in context. Upper Saddle River, NJ: Prentice Hall
- Pakman, D. (2005): Why DRM everything? A sensible approach to satisfying customers and selling more music in the digital age; Groklaw, 31 December 2005, http://www.groklaw.net/article.php?story=20051231013858642
- Rump, N. (2003): Digital rights management: Technological aspects. In: Becker et al. (2003), pp 3-15
- Smith, S.W. (2005): Trusted computing platforms: Design and applications. Berlin, Heidelberg, New York: Springer
- Stefik, M., ed. (1996): Internet dreams: Archetypes, myths, and metaphors. 3rd Printing 2001, Cambridge, MA: The MIT Press
- Stefik, M. (1996a): Letting loose the light: Igniting commerce in electronic publication. In: Stefik (1996), pp 219-253
- Stefik, M. (1999): The internet edge: Social, technical, and legal challenges for a networked world. Cambridge, MA: The MIT Press
- Stone-Lee, O. (2006): UK holds microsoft security talks. BBC, 16 February 2006, http://news.bbc.co.uk/1/hi/uk_politics/4713018.stm
- Trusted Computing Group, https://www.trustedcomputinggroup.org/home

About the author: *Robert A. Gehring* is a computer scientist specialising in issues of open source, intellectual property, and information security. He is an associate researcher with the research group for Computers & Society at the Technical University of Berlin and editor of the iRights.info consumer information website. He is co-editor of the German open source annual *Open Source Jahrbuch* and can be contacted via rag[insert at sign here]cs.tu-berlin.de.

Status: first posted 01/03/06; licensed under Creative Commons; to be included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=179

OpenTC – an open approach to trusted virtualization

By: Dirk Kuhlmann, Hewlett Packard Laboratories, Bristol, UK

Abstract: Due to the increasing complexity of IT systems, the mutual attestation of platform characteristics will become a necessity for proprietary as well as Open Source based systems. Trusted Computing platforms offer building blocks to achieve this goal. Their combination with non-proprietary virtualization technology can help to avoid much feared negative side-effects of Trusted Computing. It will permit to run locked-down execution environments in parallel with unconstrained ones, making it possible to support tight security requirements while maintaining user choice. An open approach to Trusted Computing is a prerequisite for future community based effort to describe and attest expected properties of software components in a trustworthy manner.

Keywords: project description – open source, security, trusted computing – EU

Introduction

The advent of "Trusted Computing" (TC) technology as specified by the *Trusted Computing Group* (cf. sources) has not met much enthusiasm by the Free/Open Source Software (FOSS) and LINUX communities so far. Despite this fact, FOSS based systems have become the preferred vehicle for much of the academic and industrial research on Trusted Computing. In parallel, a lively public discussion between proponents and critics of TC has dealt with the question whether the technology and concepts put forward by the TCG are compatible, complementary or potentially detrimental to the prospects of open software development models and products.

Common misconceptions of TC technology are that it implies or favours closed and proprietary systems, reduces options of using arbitrary software, or remotely controls users' computers. It has long been argued, though, that these and similar undesirable effects are by no means unavoidable, not least because the underlying technology is passive and neutral with regard to specific policies. The actual features displayed by TC equipped platforms will almost exclusively be determined by the design of operating systems and software running on top of it. With appropriate design, implementation and validation of trusted software components, and by using contractual models of negotiating policies, negative effects can be circumvented while improving the system's trust and security properties. This is the intellectual starting point of the EU-supported, collaborative *OpenTC* research and development project (project Nr. 027635; cf. sources) that started in November 2006.

Combining FOSS and TC technology

OpenTC aims to demonstrate that a combination of TC technology and FOSS has several inherent advantages that are hard to meet by any proprietary approach. Enhanced security at the technical level tends to come at the expense of constraining user options, and the discursive nature of FOSS-development could help to find the right balance here. Trusted software components have to be protected from analysis during runtime, so it is highly desirable that their design is documented and that the source code is available to allow for inspection and validation. Finally, any attempts to introduce TC technology are likely to fail without the buy-in of its intended users, and openness could prove to be the most important factor for user acceptance.

OpenTC sets out to support cooperative security models that can be based on platform properties without having to assume the iden-

tifiability, personal accountability and reputation of platform owners or users. For reasons of privacy and efficiency, these models could be preferable to those assuming adversarial behaviour from the outset. A policy model based on platform properties, however, requires reliable audit facilities and trustworthy reporting of platform states to both local users and remote peers. The security architecture put forward by the TCG supplies these functions, including a stepwise verification of platform components with an integral, hardware-assisted auditing facility at its root. In *OpenTC*, this will be used as a basic building block.

Trusted virtualization and protected execution environments

The goal of the *OpenTC* architecture is to provide execution environments for whole instances of guest operating systems that communicate to the outside world through reference monitors guarding their information flow properties. The monitors kick into action as soon as an OS instance is started. Typically, the policy enforced by it should be immutable during the lifetime of the instance: it can neither be relaxed through actions initiated by the hosted OS nor overridden by system management facilities. In the simplest case, this architecture will allow to run two independent OS instances with different grades of security lock-down on an end user system. Such a model with an unconstrained "green" environment for web browsing, software download / installation and a tightly guarded "red" side for tax record, banking communications etc. has recently been discussed by Carl Landwehr (2005). More complex configurations are possible and frequently needed in server scenarios.

OpenTC is borrowing from research on trusted operating systems that goes back as far as 30 years. The underlying principles – isolation and information flow control – have been implemented by several security hardened versions of Linux, and it has been demonstrated that such systems can be integrated with Trusted Computing technology (see e.g. Maruyama et al. 2003). However, the size and complexity of these implementations is a serious challenge for any attempt to seriously evaluate their actual security properties. The limited size of developer communities, difficulties of understanding and complexity of managing configurations and policies continue to be road blocks for deployment of trusted platforms and systems on a wider scale.

Compared to full-blown operating systems, the tasks of virtualization layers tend to be simpler. This should allow *OpenTC* to reduce the size of the Trusted Computing Base. The architecture separates management and driver environments from the core system and hosted OS instances. They can either be hosted under stripped-down Linux instances, or they can run as generic tasks of the virtualization engines. The policy enforced by the monitors is separated from decision and enforcement mechanisms. It is human readable and can therefore be subjected to prior negotiations and explicit agreement.

OpenTC chose (para-)virtualization as the underlying architecture for a trusted system architecture, which allows to run standard OS distributions and applications side by side with others that are locked down for specific purposes. This preempts a major concern raised with regard to Trusted Computing, namely, that TC excludes components not vetted for by third parties. The *OpenTC* architecture allows to limit constraints to components marked as security critical, while unconstrained components can run in parallel.

OpenTC builds on two virtualization engines: XEN and L4. Both are available under FOSS licenses and boosted by active developer and user communities. Currently, it is necessary to compile special versions of Linux that cooperate with the underlying virtualization layer. However, the development teams will improve their architectures to support unmodified, out-of-the-box distributions as well. This will be simplified by hardware support for virtualization as offered by AMD's and INTEL's new CPU generations. Prototypic results have shown that this hardware support could also allow to host unmodified operating systems other than Linux (see e.g. Shankland 2005).

From trusted to trustworthy computing

TCG hardware provides basic mechanisms to record and report the startup and runtime state of a platform in an extremely compressed, non-forgeable manner. It allows to create a digitally signed list of values that correspond to elements of the platform's Trusted Computing Base. In theory, end users could personally validate each of these components, but this is not a practical option. End users may have to rely on other parties to evaluate and attest that a particular set of values corresponds to a system configuration with a desired behaviour. In this case, their reason to trust will ultimately stem from social trust he puts in statements from specific brands, certified public bodies, or peers groups.

A much discussed dilemma arises if trusted components become mandatory prerequisites for consuming certain services. Even in case such components are suspicious to the end user, they might still be required by a provider. This problem is particularly pronounced if named components come as binaries only and do not allow for analysis. The recent history of DRM technology has shown that trojans can easily be inserted under the guise of legitimate policy enforcement modules. Clearly, a mechanism that enforces DRM on a specific piece of content acquired by a customer must not assume an implicit a permission to sift through the customer's hard disk and report back on other content.

This highlights an important requirement for components that deserve the label "trusted": at least in principle, it should be possible to investigate their actual trustworthiness. A clearly stated description of function and expected behaviour should be an integral part of their distribution, and it should be possible to establish that they do not display behaviour other than that stated in their description – at compile time, runtime, or both. A socially acceptable approach to Trusted Computing will require transparency and open processes. In this respect, a FOSS based approach looks promising, as it might turn openness into a crucial competitive advantage.

The TCG specification is silent on procedures or credentials required before a software component can be called "trusted". *OpenTC* works on the assumption that defined methodologies, tools, and processes to describe goals and expected behaviour of software components are needed. This way, it will become possible to check whether their implementation reflects (and is constrained to) their description. Independent replication of tests may be required to arrive at a commonly accepted view of a component's trustworthiness which in turn requires accessibility of code, design, test plans and environments for the components under scrutiny.

Trust, risk, and freedom

Most of us have little choice but to trust IT systems where more and more things can go wrong, while our actual insight in what is actually happening on our machines gets smaller by the day. Users are facing a situation of having to bear full legal responsibility for actions initiated on or by their machines while lacking the knowledge, tools and support to keep these systems in a state fit for purpose. Due to the growing complexity of our technology, we will increasingly have to rely on technical mechanisms that help us to estimate the risk prior to entering IT based transactions. Enhanced protection, security and isolation features based on TCG technology will become standard elements of proprietary operating systems and software in due time.

This evolution is largely independent of whether FOSS communities endorse or reject this technology. *OpenTC* assumes that mutual attestation of the platforms' "fitness for purpose" will become necessary for proprietary systems as well as FOSS based ones. The absence of comparable protection mechanisms for non-proprietary operating or software systems will immediately create problems for important segments of professional Linux users. In fact, many commercial, public or governmental entities have chosen non-proprietary software for reasons of transparency and security. These organizations tend to be subjected to stringent compliance regulations requiring state-of-the-art

protection mechanisms. If FOSS based solutions don't support these mechanisms, the organizations could eventually be forced to replace their non-proprietary components with proprietary ones: a highly undesirable state of affairs that *OpenTC* might help to avoid.

From this perspective, the current discussion about the next version of the GNU public license raises serious concerns. Some of the suggested changes could impact the possibility to combine Trusted Computing technology and Free Software licensed under GPLv3 - this refers to the GPLv3 Draft, status 2006-02-07 16:50 (cf. sources). Section 3 of this draft concerns *Digital Restrictions Management*, a term that has been used by Richard Stallman in discussions about Trusted Computing. For example, the current draft excludes "*modes of distribution that deny users that run covered works the full exercise of the legal rights granted by this License"*. It is an open question whether this might apply to elements of a security architecture such as *OpenTC*. A Trusted Computing architecture does not constrain the freedom of copying, modifying and sharing works distributed under the GPL. However, it can constrain the option running modified code *as a trusted component*, since previously evaluated security properties might have been affected by the modifications. Unless a re-evaluation is performed, the properties of modified versions can not be derived from the attestation of the original code; security assurances about the original code become invalid.

This is by no means specific to the Trusted Computing approach; it also applies to commercial Linux server distributions with protection profiles evaluated according to the Common Criteria. The source code for the distribution is available, but changing any of the evaluated components results in losing the certificate. Whether or not software is safe, secure, or trustworthy is independent of the question of how it is licensed and distributed. The option to choose between proprietary and FOSS solutions is an important one and should be kept open. This is one of the reasons why several important industrial FOSS providers and contributors participate in *OpenTC*. The project aims at a practical demonstration that Trusted Computing technology and FOSS can complement each other. This is possible in the context of the current GPLv2. Whether it will be so under a new GPLv3 remains to be seen.

Sources

- GPLv3 Draft, status 2006-02-07 16:50: http://gplv3.fsf.org/draft
- Landwehr, Carl (2005): Green Computing. IEEE Security&Privacy, Vol 3, Nr 6, Nov/Dec 2005, p. 3
- Maruyama et al. (2003): Linux with TCPA Integrity Measurement. IBM Research Report RT0575, January 2003; http://www.research.ibm.com/trl/people/munetoh/RT0507.pdf
- OpenTC: http://www.opentc.net
- Shankland, Stephen (2005): XEN passes Windows Milestone. CNET News.com, August 23, 2005; http://news.com.com/Xen+passes+Windows+milestone/2100-7344_3-5842265.html
- Trusted Computing Group: http://www.trustedcomputinggroup.org

Disclaimer

The content of this paper is published under the sole responsibility of the author. It does not necessarily reflect the position of HP Laboratories or other OpenTC members

About the author: *Dirk Kuhlmann* is a senior research engineer for Hewlett Packard Laboratories in Bristol, UK, where he works as a member of the Trusted Systems Laboratory. He acts as the overall technical lead for the OpenTC project. Contact: dirk.kuhlmann@hp.com

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=183

The role of Trusted Computing in Digital Rights Management within the OpenTC project

By: Florian Schreiner, Michael Pramateftakis and Oliver Welter, Institute for Data Processing, Munich University of Technology, Munich, Germany

Abstract: Much of the negative impression of DRM comes from the fact that current systems offer very little transparency and convenience to the user. Within the OpenTC project, we pursue an approach for DRM towards the introduction of a standardised license-processing core that is open to the public and common to a variety of DRM-related applications. We hope that the trusted environment, in which the DRM core and applications are executed, together with the open architecture, will help to introduce clarity and convenience in the DRM process and thus give a positive spin to the topic.

Keywords: technical analysis – DRMS, MPEG-21, OMA, trusted computing

Introduction

Digital Rights Management (DRM) systems govern the use of content by describing per-user rights in machine-readable licences and enforcing them by using cryptographic methods. The public's conception of the term "DRM" today does not extend beyond a copy-protection system of the content industry. DRM systems are seen as means to just restrict copying and sharing of multimedia content and are thus viewed negatively.

The OpenTC project will provide an open-source framework for establishing trusted application environments on free operating systems like Linux. This approach plans to enforce integral trust and security of the system, because the applications are caged in trusted environments, in which only certified, trustworthy applications are allowed to run. The system can detect malicious software like viruses and exploits and prevents their execution. Furthermore, OpenTC protects imperilled programs against external access, so that no program outside the environment may access security relevant data. The trust is rooted on a Trusted Platform Module (TPM), a hardware component that can securely store cryptographic keys and ensure integrity of the system.

We aim to use this concept for creating a DRM system which governs the use of all kinds of sensitive data, not just multimedia content. An example for alternative uses of DRM is the medical sector, where patient records and related information have to be protected against unauthorised access. Without a trusted environment, attackers may enter a computer system e.g. by using a virus or exploiting a security vulnerability to obtain unauthorised access to stored information, including sensitive data. In a trusted system, sensitive information is protected by encryption. The corresponding keys are stored within the TPM and are bound to a specific platform state (This procedure is called "sealing" in the Trusted Computing Group nomenclature). Rogue software is never allowed to be executed in a trusted system and even if it were, it would alter the platform's state, thus disabling access to the "sealed" keys.

A trusted infrastructure on an open-source system may open the door for devising DRM systems providing two primary advantages: Transparency and interoperability. By introducing an open DRM core that is common to all applications, the DRM procedure becomes more transparent. This is in strong contrast to the current situation, where security is mainly based on obscurity, i.e. on keeping the function of the DRM system itself secret. This leads to proprietary applications to handle protected content and as a direct consequence thereof those applications preclude interoperability. Accordingly, many different systems and applications exist for performing the same task, each one having its own ways for managing content and licenses. In contrary to that, an open architecture facilitates interoperability, because the DRM core uses standardised technology for

license management. Various elements of the MPEG-21 standard will be used to accomplish this mission. Internally, the DRM core works with MPEG-21, so whenever licenses from external licensing domains are introduced to the system, e.g. licenses issued by OMA DRM or Windows Media DRM, the DRM core translates them into an equivalent MPEG format so it can manage them. Such translations, although technically feasible, are facing trust problems. Since licenses are signed by the content owners or rights holders, a translated license must also be signed by a trustworthy entity. Such a signature is only possible when a trusted environment is present, like the one provided by OpenTC. The trusted environment is also beneficial in cases where content reencryption is needed.

MPEG-21 Rights Expression Language (MPEG REL) is a language versatile enough to accommodate functionality from various other rights expression languages. Thus, translations to and from other languages are possible, as long as they are based on the same principles. Such translations are needed when content needs to be transferred to external devices for rendering. The procedure can be made transparent to the user, who does not have to deal with trust issues, as they are automatically taken care of by the DRM core.

A concept for an interoperable DRM system

Our concept is based on several services that we can expect from the OpenTC infrastructure: The TPM-Chip is the root of trust in the system and is used by OpenTC for building up a trusted environment for applications. Only certified applications are allowed to run in such a context and they can rely on the fact that the underlying operating system with its modules and drivers are trusted, too. We assume that all data within the secure environment is protected against attacks, so no special care or encryption in the user layer is necessary any more. The distributor of the operating system decides which program is secure and which not, and provides relevant certificates. These certificates may also contain information about the capabilities of the application or the level of security it needs to perform particular actions. Depending on this information, OpenTC can restrict access to sensitive information or specific hardware components of the system. Thus, uncertified applications, including viruses, manipulated hardware drivers and other malicious code cannot start in a secure environment. This protection is transparent to the user, as the OpenTC infrastructure takes care of it in the background without the need for user intervention.

The diagram next page shows our currently planned architecture with the above environment in mind:

The central component of the system is the DRM-Core. Its tasks are to offer several services to the application layer regarding interpretation of licenses, as well as to provide the central key store for protected content. As it is a component used by several applications, it is placed within the OpenTC infrastructure. That way, it can be certified along with the system and be trusted by all applications. The Core consists of three basic parts: The license parser, the translation manager and the key store.

License Parser

The License Parser offers services regarding verification and interpretation of licenses. These services are central to any DRM process and are accessed from the outside by an API, which includes all functions that are necessary for an application to access a protected file. A player application can be any program that can be executed in a trusted environment and that is able to render content. It has to be compatible to the DRM-System to know the API of the core and how to handle content. Such a player application can directly access the DRM-Core via the API to request access to protected content. The player has to provide its license, so the core can decide if the user has permission to access the data. If access is granted, the core returns the content key from the key store and the player can render the content. Legacy players, which cannot access the API directly, are also supported by our architecture. Players of that kind are not aware of the DRM-Core, but are favoured by users for whatever reason. These cases are handled by an IO-Socket interface, which handles the

license authentication and interpretation transparently to the application. For the player, the whole process is similar to a normal file access. The player only has to support the content's type and be connected to the IO-Socket through a plug-in. The player receives the unprotected content from the socket and can render it. The IO-socket in this case converts and forwards requests through the API to the DRM-Core. Since all applications, including the legacy ones, run in the secured environment, handing out the content key or the decrypted content itself is no problem, since it is guaranteed that the applications will not misuse it. This is a great advantage of having a trusted computing base.

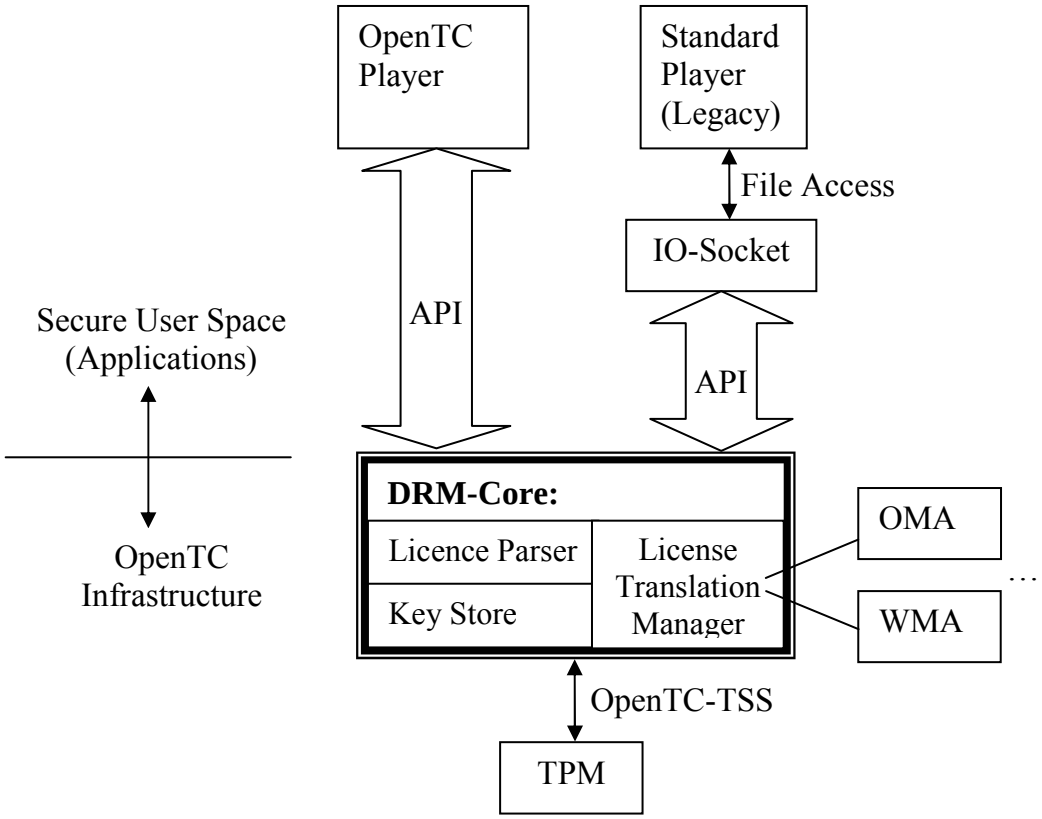


Figure 1: Diagram of currently planned architecture

License Translation Manager

Internally, the core uses MPEG-21 as a DRM framework. MPEG-21 also provides facilities for identifying content. Unique identifiers are used by the core to relate content with licenses and keys in the key store. Whenever foreign content enters the system, i.e. content protected with a license in a language other than MPEG REL, the license translation subsystem converts the external license to MPEG REL, so that it can be processed by the license parser. Since the core is trusted, the translation can also be trusted. The license translator uses an extensible architecture which utilises plug-ins for different license formats. Our prototype will support at least OMA licenses, while other common ones, e.g. Windows Media and iTunes, can also be supported if respective information is available. The translation manager can be requested to export an MPEG license into any other supported format. The import/export functionality of the DRM-Core provides interoperability with other systems.

Key Store

A particularly important component of the core is the key store. The key store contains

the keys which were used to protect content in the system. The core ensures that a content key is given out only when a requested action is allowed by the license. The key store is organised as a table which contains keys and unique content identifiers. The same identifiers are used in the licenses to reference content. Respective technologies are part of the MPEG-21 standard. The key store is implemented as an encrypted file, which is decrypted by the core when a secure environment is established. This is done with the help of the TPM, which seals the key store master key, so that it can only be accessed in a particular system integrity state. The core itself is thus only able to retrieve the master key when the system is secure.

Discussion

Multimedia content is used in a variety of industrial branches. As described above, the health sector is a good example for the reasonable usage of a DRM system. Another application is in the entertainment sector, where video and audio files need protection. In that case, the system provides fairness towards the user as well as to the owner of the content. In the e-learning sector the system can be used as a cheap and standardised solution to protect important multimedia content. The standardisation enables the system to work on different platforms, a fact that is useful in teaching facilities with large heterogeneous networks.

We believe that by using the advantages a trusted computing environment provides, we can develop a successful DRM-System. The important advantages our system will have are:

- Interoperability with other DRM Systems
- Transparency
- Convenience for the user
- Support of legacy software

Our approach differs from other DRM-Systems, because it will be open-source and uses the TPM-Chip to enforce security. Today, many systems are obscure and it is essential for them to keep the encryption methods secret. In contrast to that, open source means that every user can observe exactly what happens with the licenses and the keys. In combination with the TPM-Chip a secure and trustworthy system can be designed, which enforces all applications to work according to their specification. Security is then based on the manufacturer of the TPM-Chip, who ensures and certifies that it is a trustworthy hardware component.

In our project we also would like to involve the Open Source Community. Generally, we expect a negative reaction because our system works basically as a usual DRM System. The Draft version of the GPLv3 gives an impression about the emotional attitude towards DRM. In our point of view the principal problem of DRM is that it is not transparent enough for the user. But this is not a technical problem; it is an effect of the marketing and business models behind the content. These models are so restricted that user interference is often needed.

We hope that participation of the Community in our project will improve such problematic aspects. The project will be available under the GPL, so that the system can even be extended by the open-source community if the need arises. In that way, we want to enable the Linux community to use the advantages of Trusted Computing based DRM for protecting arbitrary data.

Sources

- MPEG: MPEG-21 Multimedia Framework Part 1: Vision, Technologies and Strategy.
  Reference: ISO/IEC TR 21000-1:2004. From ISO/IEC JTC 1.29.17.11
- MPEG: MPEG-21 Multimedia Framework Part 3: Digital Item Identification.
  Reference: ISO/IEC TR 21000-3:2003. From ISO/IEC JTC 1.29.17.03
- MPEG: MPEG-21 Multimedia Framework Part 4: Intellectual Property Management and Protection Components.
  Reference: ISO/IEC TR 21000-4. From ISO/IEC JTC 1.29.17.04
- MPEG: MPEG-21 Multimedia Framework Part 5: Rights Expression Language.
  Reference: ISO/IEC FDIS 21000-5:2004. From ISO/IEC JTC 1/SC 29/WG 11

- MPEG: MPEG-21 Multimedia Framework Part 6: Rights Data Dictionary. Reference: ISO/IEC TR 21000-6:2004. From ISO/IEC JTC 1.29.17.06
- Open Mobile Alliance (2005): DRM Specification Candidate Version 2.0. http://www.openmobilealliance.org/release_program/drm_v2_0.html
- OpenTC-Project Homepage: http://www.opentc.net/
- Trusted Computing Group (2004): TCG Specification Architecture Overview. Trusted Computing Group, Incorporated. Revision 1.2

About the authors: Dipl.-Ing. *Florian Schreiner* is a research and teaching assistant at the Institute for Data Processing, Technische Universität München. Contact: schreiner@tum.de

Dr.-Ing. *Michael Pramateftakis* is a research and teaching assistant at the Institute for Data Processing, Technische Universität München. His research field is system security and cryptography. Contact: pramateftakis@tum.de

Dipl.-Ing. *Oliver Welter* is a research and teaching assistant at the Institute for Data Processing, Technische Universität München. His research field is public key systems and their application. Contact: welter@tum.de

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=184

iPod's hegemony challenged

New music-enabled smart phones enter the market

By: Gergely Tóth, SEARCH Laboratory, Budapest, Hungary

Abstract: The upcoming version of the Symbian operating system for mobile phones – announced for the Nokia N91 and the Sony Ericsson W950i multi-media phones – introduces Trusted Computing based security features like secure software installation and restricted data storage locations – core requirements for a secure DRM platform. On the other hand, the main novelty of these phones is their 4 GB internal hard disk directly aiming for mass music storage. This step marks the dawn of real music-enabled mobile phones. However isn't it too late to compete with Apple's iPod?

Keywords: news analysis – DRMS, music markets, security, trusted computing

Introduction

Symbian is the operating system of a wide variety of so called smart mobile phones providing an open development environment for different mobile vendors and mobile operators. As of December 2005, worldwide shipments of Symbian OS phones reached 58.8 million phones (source: Symbian website).

The newest version of the operating system, version 9.1 is just about to appear in commercially available mobile phones. Both Nokia and Sony Ericsson have announced phones based on this version, most notably the Nokia N91 and the Sony Ericsson W950i type. While one of the most important novelties of the new OS is a Trusted Computing based security model (especially suitable for DRM), the main customer-attracting function is to act as an easily usable music player – undoubtedly an attempt to gain a foothold in the Apple iPod-dominated market segment.

In this article first the Trusted Computing based security model of Symbian v9.1 will be introduced, then I will evaluate the possibilities of using v9.1 for DRM, and finally I will look into the chances of the music-enabled phones to become real competitors of the iPod.

Platform security in Symbian OS

The implementation of the Trusted Computing concept in the new Symbian operating system is called Platform Security and its main security functions are the following:

- In the **capability model** so called capabilities (similar to permissions) are assigned to groups of sensitive operations (e.g. network access, PIM access, local connectivity or camera access). Only processes having the corresponding capabilities can carry out the given sensitive operation.

  Capabilities are grouped: the most critical (e.g. access to all files of the phone) form the Trusted Computing Base (TCB), which allows full access to all system resources; the Trusted Computing Environment (TCE) comprises capabilities for selected system services and finally all other capabilities are user-visible. Naturally, only a small, highly trusted group of applications will have TCB capabilities, most programs will only have user visible capabilities at most.

- Symbian v9.1 incorporates a **secure software installation mechanism**: only digitally signed applications can be installed. The set of capabilities assigned to the applications is included in the installation package (also protected by the signature) and cannot be altered. The signatures are centrally issued (by Symbian, see SymbianSigned, or by the vendor or operator) only after the developer has been reliably identified and the need for the required capabilities is justified.

  A crucial property of v9.1 is that applications cannot be modified after they have been installed – the kernel (i.e. the system's innermost core) ensures that the location of executable applications is read-only, thus only what has been digitally signed can run on the phone. This means that no third party program can be run on the system with crucial capabilities without prior authorization, thereby mitigating the chance that hackers gain access to the system and also the possibility of virus spreading can also be effectively limited.

- Finally, the OS enforces **separation of the applications and processes**. During run-time applications cannot access each other's memory area except for carefully guarded inter-process communication, whereas for persistent storage each application may create a private directory to which only that application has access. This technique is called data caging, so storing sensitive data in private directories applications can protect their assets from other applications and therefore even against the user himself.

With these new features Symbian took a large step forward providing a secure mobile platform – a risky undertaking considering that the new architecture broke compatibility with the old one, thus previous applications of Symbian v6 and v7 will not run on v9.1. It remains to be seen whether this change was worthwhile, only time will tell the real strength of the architecture since there are currently no devices on the market with Symbian OS v9.1 and thus it has not yet been tested by the community.

DRM based on platform security

Although the aim of Platform Security was not mainly to provide a secure architecture for Digital Rights Management, Symbian v9.1 surely is a starting base for DRM:

- Due to the secure **software installation mechanism** and the **capability model** (as DRM is also guarded by a dedicated capability) only digitally signed and designated applications can access DRM services thus limiting the possibility of unauthorized access. The fact that only tested, signed (and thus back-traceable) applications are allowed to run on a phone is also in favour of DRM.
- On the other hand **data caging** is especially useful for storing secret DRM information (e.g. keys or usage count for limited access assets), since only the dedicated DRM application has access to these pieces of information and thus the secrets can be effectively hidden from unauthorized parties.

These special functions make Symbian v9.1 a safe choice to implement a DRM system.

Music players based on Symbian v9.1

In 2005 Nokia announced the N91 music-enabled mobile phone with 4 GB internal storage for multimedia files. Sony Ericsson soon followed with the W950i, which has similarly 4 GB of space for multimedia. Although neither of them is available on the market yet, both are planned to have Symbian v9.1 as the operating system. While it is yet unsure what DRM solutions W950i will support, Nokia has already announced full OMA DRM 2 and Windows Media DRM 10 support for N91.

Up till now mobile phones on their own did not have enough capacity to store a reasonable amount of music files internally, and only high-end models were outfitted with some sort of memory card slots to be able to play music files from removable storage. This was clearly inferior to Apple's various iPod versions where the smallest version has 1 GB internal storage capacity (and larger ones going up to 60 GB). With this first step of 4 GB internal drives the mobile vendors demonstrate their decision to enter the market of portable music players. What can be the advantages of such devices against the market-dominant iPods?

- First of all these devices are not just music players, they are fully featured **smart phones** with a wide variety of functions ranging from office applications, PIM services to naturally all kinds of connectivity (GSM, GRPS, 3G, Bluetooth and sometimes even W-LAN etc.).
- Secondly, Nokia has already demonstrated the will to support multiple DRM formats (namely OMA DRM2 and Windows Media DRM 10). This will not only attract content providers but also customers as music from different platforms can be accessed and shared. Many surveys clearly showed that **interoperability** is a key advantage in case of DRM solutions.
- Finally, Symbian-based platforms have a **reputation of being secure** – whereas installing a custom OS onto iPod has a lively community (see the iPodLinux homepage) and the Fairplay DRM system has already been circumvented (Orlowski, 2004), cracking or re-flashing a Symbian-based phone has not yet been demonstrated in public.

All these advantages and the ease of usage will compete with the dominance of iPod and iTunes.

Bottom line

Apple's dominance with the iPod music player on the market is unquestionable; however the competition is slowly starting to react. The newest potential rivals arrive in the form of smart phones with 4 GB of internal storage for music files. The device from both Nokia and Sony Ericsson are based on the upcoming operating system of Symbian with enhanced security functions based on Trusted Computing. The applicability of such phones for DRM-based solutions is obvious, thus support from content providers can be anticipated, and their rich feature set may provide them with an advantage over the iPods. The question is whether the market will also appreciate these devices and how the different DRM solutions will be affected – could it be that this new competition will enforce their interoperability?

Sources

- Symbian OS – the mobile operating system, London, UK: http://www.symbian.com
- Nokia Nseries N91 – http://www.nokia.com/n91
- Sony Ericsson W950i – http://www.sonyericsson.com
- SymbianSigned – http://www.symbiansigned.com
- Apple iPod – http://www.apple.com/ipod
- iPodLinux – http://www.ipodlinux.org
- Orlowski, A (2004).: New workaround for Apple DRM, The Register, April 6, 2004; http://www.theregister.co.uk/

About the author: *Gergely Tóth* is a researcher at SEARCH Laboratory, Budapest, Hungary. Besides Digital Rights Management his core interests include security and privacy. Please visit http://www.planeforge.com/home/tgm.

Status: first posted 02/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=185

Legal risk assessment of Trusted Computing. A review

By: Arnd Weber, ITAS, Karlsruhe, and Dirk A. Weber, IT-Consultant, Bad Homburg, Germany

Abstract: In this article, potential legal issues of Trusted Computing are presented as discussed by legal scholar *Stefan Bechtold*. This review not only summarizes the main risks identified by Bechtold, but tries to add to the debate.

Keywords: review – copyright law, DRMS, privacy, secure operating system, trusted computing.

Introduction

The main article reviewed here is "Trusted Computing. Rechtliche Probleme einer entstehenden Technologie" ("Legal problems of an emerging technology"; Bechtold 2005b). This article is based on a presentation given at the U.S. Stanford University in March 2005, the slides and talk of which are available in English (2005a). Bechtold published a slightly updated version of his article, again in German (2005c). There is also a further article on TC taken into account for this review (2004b) referring to a somewhat earlier stage of TC-developments.

The reasons for this review is that Bechtold provides quite a dense and comprehensive assessment of potential legal problems associated with Trusted Computing, in particular in the area of DRM. Areas in which legal problems might emerge are identified, and recommendations are given to policy makers and those building "Trusted Computing" systems.

Background of Trusted Computing

"Trusted Computing" is a notion used by the "Trusted Computing Group" (TCG), which emerged from the former TCPA, the Trusted Computing Platform Alliance, which was founded in 1999. At that time, there had been discussion whether computers should have identifiers (cf. the discussion about the Personal Serial Number in the Intel Pentium-III processor; STOA 1999). As the TCPA suggested to have a unique identifier in each "Trusted Platform Module", observers were worried that it might be aimed at tracing PC users in general, as opposed to using the identifier only for purposes such as identifying parties in electronic commerce. When Microsoft considered using the Trusted Computing approach for basing a DRM-system, "TC" obtained a somewhat negative image in many popular media, blogs, etc. Today, the TCG is led by AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft and Sun.

Key security concepts in the TCPA specifications were based on work by Arbaugh et al. (1997). The process the authors designed is "constructing a chain of integrity checks, beginning at power-on and continuing until the final transfer of control from the bootstrap components to the operating system itself. The integrity checks compare a computed cryptographic hash value with a stored digital signature associated with each component" (Arbaugh et al. 1997). In TCPA/TCG implementations, the chain of trust starts accordingly with the "Trusted Platform Module" (TPM), basically a smartcard chip. Today, TPMs in PCs are mainly used for secure log-in, protection of cryptographic keys, and file encryption support. Checking the whole chain of trust, e.g., operating system, drivers and applications, has not yet been implemented.

The subject of Bechtold's analysis

Bechtold reviews the actual specifications written by the Trusted Computing Group, as

well as operating system developments, such as Microsoft's "Next Generation Secure Computing Base" (NGSCB; variants of new Microsoft operating systems will increasingly support applications based on TC concepts). In addition, he takes into account recent hardware developments, in particular the new processor architectures from Intel and AMD that offer support for "curtained memory " and "virtualization". Curtained memory allows for strong isolation between different execution environments, while virtualization allows several different, even unmodified operating systems to run in parallel. Next to a legacy OS, another one could run, e.g. a custom-made one for a content application. With the help of the TPM, it can be determined what is actually running.

The following potential characteristics of Trusted Computing are highlighted:

1. Remote attestation: Comparison of the actual state of a platform with its expected state (validation).
2. System compartmentalisation: With the new processor architecture, e.g., a Trojan horse would not longer be able to read data from a banking application, as these would run in different compartments.
3. Sealed storage: Data are encrypted and can only be read if the system is in a certain state (for making sure that, e.g., no software is running which is designed to "rip" content).
4. Secure input/output: Keyboard, mouse and display are protected against manipulation.

From this list, we see that in frequent cases envisaged by the proponents of TC, "trusted" means that a third party can be enabled to check whether a remote computer can be trusted. Whether a "trusted computer" is trusted by the user, can deserve to be called "trustworthy", etc. is a different matter. As Pearson, editor of an early book on TC, put it when describing the TPM: "This security hardware contains those security functions that *must* be trusted." (2003, p. 5; emphasis in the original). Whether it is trusted in social and economic terms, is a different matter, however.

Risk analysis

Generally speaking Bechtold argues that there are possibly many risks arising, but that they could be dealt with by skilful design of TC-architectures and the institutional arrangements around them. We pick up here the most important points in slightly more detail:

- Remote attestation could be used to hinder inter-operability. It could be ensured that only a certain piece of software, e.g. a Microsoft browser, can be used for getting certain services. He discusses technical remedies such as communicating only properties of a program, or attesting only the correctness of small part of the computer, e.g., a compartment, as well as legal remedies to prevent abuse of market power.
- The role of third parties providing basic keys and metrics for using TC is an issue. For instance, the integrity of software might be checked by comparing its hash value against the one it is supposed to have. Currently, the TCG specifications do not define who these entities will be. It could be, for instance, a large corporation doing it in its own interest. However, central authorities could emerge with a significant market power. Therefore it is of potential relevance that there will be several competing companies or organisations certifying such data.
- Given the market power of dominant players such as Microsoft, the article argues, users might be forced to use TC. For instance, banks might require the use of TC. The author demands to take such dominance, or market failures, into account.
- "Sealed storage" might be used to ensure that certain data formats need to be used. Trusted Computing "can be used to 'seal' data to a particular software state on a platform. In a DRM system, this feature could be used by content providers to make sure that their content may only be accessed by consumers if their devices are in a secure state. However, it could also be used to seal data to a particular operating system, platform configuration,

or software application. Software companies could develop proprietary file formats for their applications that can read this file format and thereby interoperate. As the costs of converting files would be significantly increased, this could deter customers from switching to competing applications, operating systems and even hardware platforms in the first place. Content providers could make sure that their content is only accessible with a particular proprietary player. In general, sealed storage could hamper competition in the hardware, operating system and the software applications markets. Trusted computing could prove a powerful tool to create customer lock-in and artificially increase switching costs." (2004b, p. 88f). Competition law would be a way to deal with the issue.

- TC could be used to design a highly secure DRM system which would be difficult to circumvent. TC could be used to prevent the computer user from copying content from one system to another, as more easily possible with other DRM systems. He concludes that "DRM systems which are based on trusted computing architectures may come into conflict with copyright law... If copyright limitations allow a consumer to copy content to another device without the rights holder's permission, the trusted platform could nevertheless prevent such copying as the sealed content could not be decrypted on the other device." (2004b, p. 95)
- The use of keys could lead to a loss of privacy. Not only could a company verify whether one of its PCs is accessing its network, other companies could also identify platforms and concatenate keys and user identities. Bechtold reviews the merits of "Privacy Certification Authorities" providing pseudonyms and so-called "Direct Anonymous Attestation" which could be used to provide a higher level of anonymity (cf. TCG 2003).

The article also addresses other issues, such as using related patents to limit competition.

Discussion

The reader gets the impression that Bechtold intends to warn of potential negative effects. In contrast to earlier such warnings, e.g. Ross Anderson's, he separates issues of TC (according to the TCG specifications), Microsoft's plans, and DRM very clearly (cf. Safford 2002). In this sense, his work is a very useful early warning.

Summarising one can say that there are three major risks:

1. Dominance of players. This could result in high prices, and in particular the use of open source software could be hindered if certificates were made available only with a delay or at excessive cost.
2. Loss of capabilities to exploit copyright limitations.
3. Loss of privacy.

These could be addressed by the following remedies:

1. Remote attestation could be requested from only a small part of a computer, e.g. a compartment.
2. Competing operating systems and competing institutions providing keys and hash values would be necessary for consumers to have a choice. Thus, a possible abuse of market power would be hindered. With enough competition, applications not using TC would also remain available.
3. Control of abuse of market power through the policy maker.
4. Privacy Certification Authorities and Direct Anonymous Attestation could be deployed to provide more privacy.

With respect to the design of DRM systems Bechtold believes in "value centered design" enabling DRM-implementations preserving copyright limitations, such as private copies (cf. 2004a).

The reviewers would like to bring up a few issues for discussion:

First, Bechtold has a fairly short list of positive effects, essentially stating that digital signatures could be implemented more securely. Other potential effects of TC, such as

increased security against theft of data, e.g. from stolen laptop computers, are underemphasised. Also the potential of secure computers to make fighting malicious code less important is underemphasised. But elaborating on such benefits was apparently not within the scope of his article.

Second, Bechtold seems to have the impression that all the hard- and software which is envisaged to be built based on the TCG-principles will work properly. This may not be the case, however. It is by no means guaranteed that it will be possible to implement all the functions in an error-free way. He writes, e.g., that existing PC-architectures need only be "marginally modified" (2005b, p. 394), or that "Trusted Computing will offer a much higher level of security" (p. 404) or that "it is impossible for insecure software, viruses and other dangerous programs to hide their existence on a Trusted Computing-platform" (p. 399). This will only be the case if TC is implemented perfectly. In particular, it seems doubtful whether a permanent attestation is feasible. If attestation is not permanent, but e.g. takes place only during the system's boot process, malicious code, cracking software, etc., might run even in a verified compartment. Regarding DRM, there is also the challenge to build PCs which make it difficult to eavesdrop data somewhere. Applying the BORA principle, cracked content could run undetected in a future, separate compartment. Protections such as watermarking might perhaps remain, though, and the process might be illegal, which would reduce such abuse.

Third, there is the interesting issue whether Microsoft will aim at blocking virtualisation regarding non-Microsoft operating systems and compartments. New Microsoft operating systems could ensure, with the help of the TPM, that they only run if no other compartments with different operating systems are running. This would hinder competition.

Bottom line

One could regard Bechtold's worries as an example of German thoroughness and of scepticism with regard to new technologies. It seems, however, his work is right in time, as there is a good possibility that during the next few years hundreds of millions of TPMs will be in PCs. Therefore it is important to monitor whether Trusted Computing will lead to secure systems, or to lock-in. Regarding DRM, Bechtold warns that TC might prevent users from exploiting rights provided by the copyright law, so this issue will also warrant continued monitoring.

Sources

- Anderson, Ross (2005): Trusted Computing. Frequently Asked Questions. Access 16.12.2005. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
- Arbaugh, William; Farber, David; Smith, Jonathan (1997): A secure and reliable bootstrap architecture. In: Proceedings of the 1997 IEEE Symposium on Security and Privacy, pp. 65-71; http://www.cis.upenn.edu/~waa/aegis.ps
- Bechtold, Stefan (homepage): http://www.bechtold.name/
- Bechtold, Stefan (2004a): Value-centered design of Digital Rights Management. INDICARE Monitor, Vol. 1, Number 4, September 2004; http://www.indicare.org/tiki-read_article.php?articleId=39
- Bechtold, Stefan (2004b): Trusted Computing Initiatives – Protecting virtual Troy or creating a Trojan horse? In: Koenig, Christian; Neumann, Andreas, Katzschmann, Tobias: Trusted Computing. Technik, Recht und gesellschaftspolitische Systemumgebungen. Heidelberg 2004 pp. 77-99
- Bechtold, Stefan (2005a): Trusted Computing: Whom do we trust? Presentation given at Stanford Law School, March 2005. Slides and talk available at: http://cyberlaw.stanford.edu/events/archives/stefan_bechtold_2005.shtml
- Bechtold, Stefan (2005b): Trusted Computing. Rechtliche Probleme einer entstehenden Technologie. In: Computer und Recht 6/2005, 393-404 (2005b)
- Bechtold, Stefan (2005c): Update of Bechtold 2005b; http://cyberlaw.stanford.edu/blogs/bechtold/tcblog.shtml
- Intel (2003): LaGrande Technology Architectural Overview. http://download.intel.com/technology/security/downloads/LT_Arch_Overview.pdf
- Pearson, Siani (ed.) (2003): Trusted Computing Platforms. TCPA technology in context. Upper Saddle River 2003

- Safford, David (2002): Clarifying Misinformation on TCPA. IBM Research 2002; http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf
- STOA (Scientific and Technological Options Assessment) Panel, European Parliament: Development of Surveillance Technology and Risk of Abuse of Economic Information. Luxembourg, April 1999; http://www.cryptome.org/stoa-r3-5.htm
- Trusted Computing Group (2003): TPM v1.2 Specification Changes. October 2003. https://www.trustedcomputinggroup.org/

About the authors: *Arnd Weber*, researcher at ITAS, is currently participating in the OpenTC project (http://www.opentc.net). Recent research addressed success factors of the Japanese mobile data (and music) market. He has also done work on "secure wallets" in the framework of EU-projects CAFE and SEMPER. *Dirk A. Weber* has experience with managing corporate networks as a Microsoft Certified Systems Engineer and as a Certified Novell Engineer. Contact: arnd.weber@itas.fzk.de and dirk.weber@compuserve.com.

Status: first posted 02/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=186

Masthead

The INDICARE Monitor is an electronic periodical of the EU-funded project INDICARE being published every last Friday of a month. Articles having passed an internal review process are immediately posted at the INDICARE homepage for public debate. Authors are encouraged to revise their articles in the light of previous discussion before publication in the monthly issue.

- You can use the *RSS-feed* to get articles as soon as they are posted.
- You can *subscribe* to the INDICARE Monitor, and receive an *e-mail notification* containing the contents page (title, author, abstract, and URLs) and a link to the pdf-version (this service replaces the bi-weekly INDICARE newsletter). Just type in your e-mail address at the INDICARE Website and Go!, or send an empty e-mail to: indicare-monitor-subscribe@indicare.org
- The *INDICARE Monitor Archive* offering all issues in HTM and PDF is available at http://www.indicare.org/tiki-page.php?pageName=IndicareMonitor
- The *INDICARE Homepage*: http://www.indicare.org/

Editorial policy: The INDICARE Monitor is an English language periodical publishing original works. The editorial policy attempts to be balanced, unbiased, neutral, and non-partisan, not excluding however provocative, pointing and sometimes even lopsiding contributions. Articles are written by INDICARE staff and external experts. The style is intended to be analytical, concise, compact, and written in a language comprehensible for non-experts. The expected length of an article is between 5000 and 10.000 characters. The INDICARE Monitor is available for free.

Disclaimer: The views and opinions expressed in the articles of INDICARE Monitor do not necessarily reflect those of the European Commission and the INDICARE consortium or partners thereof. All articles are regarded as personal statements of the authors and do not necessarily reflect those of the organisation they work for.

Acknowledgment: The INDICARE Monitor is an activity of the INDICARE project, which is financially supported as an Accompanying Measure under the eContent Programme of Directorate General Information Society of the European Commission (Reference: EDC - 53042 INDICARE /28609).

Contact

Knud Böhle (Editor)
Institute for Technology Assessment and Systems Analysis (ITAS)
Phone: +49 (0)7247/82-2989 (-2501)
Fax : +49 (0)7247/82-4806
E-Mail: knud.boehle@itas.fzk.de

Keyword Index

This index helps to find articles by *article-type*, subject matter and regional focus.

Name Index

This index references names of persons – not including deliberately names of authors.