Nora Weinberger, Arnd Weber, Sven Reisch

ITA-Monitoring

„Klebrige Informationen“

Pre-Print: 06.12.2011

Erschienen in: Decker, M.; Fleischer, T.; Schippl, J.; Weinberger, N. (Hrsg.): Zukünftige Themen der Innovations- und Technikanalyse. Methodik und ausgewählte Ergebnisse. KIT Scientific Reports 7605. Karlsruhe: KIT Scientific Publishing 2012, S. 121-169

ITAS – Elektronische Pre-Prints

Allgemeine Hinweise

Wie mittlerweile viele wissenschaftliche Einrichtungen, bietet auch ITAS elektronische Pre-Prints an, die bereits zur Publikation akzeptierte wissenschaftliche Arbeiten von Mitarbeiterinnen und Mitarbeitern - in der Regel Buchbeiträge – darstellen.

Für die Autoren bietet dies den Vorteil einer früheren und besseren Sichtbarkeit ihrer Arbeiten; für die Herausgeber und Verlage die Möglichkeit einer zusätzlichen, werbewirksamen Bekanntmachung des jeweiligen Buchprojekts. Auf die in Aussicht stehende Veröffentlichung wird hingewiesen. Nach Erscheinen der Publikation werden der geänderte Status vermerkt und die bibliographischen Angaben vervollständigt.

Allgemeine Anregungen und Kommentare zu den ITAS Pre-Prints richten Sie bitte an (info@itas.kit.edu).

Empfohlene Zitierweise des vorliegenden Pre-Prints:

Weinberger, N.; Weber, A.; Reisch, S.:
ITA-Monitoring „Klebrige Informationen“ (Kurzstudie).
Karlsruhe: ITAS Pre-Print: 06.12.2011;
http://www.itas.fzk.de/deu/lit/epp/2011/weua11-pre01.pdf

Karlsruher Institut für Technologie

ITA-Monitoring „Klebrige Informationen“

Kurzstudie

Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des Karlsruher Institut für Technologie (KIT)

Oktober | 10

Projektleiter: Prof. Dr. Michael Decker

Autoren: Nora Weinberger (ITAS, KIT),Arnd Weber (ITAS, KIT), Sven Reisch (ITAS, KIT)

Inhaltsverzeichnis

Danksagung

Die Autoren möchten die wertvollen Beträge der interviewten Expertinnen und Experten anerkennen: Hannes Federrath, Christine Hafskjold, Matthias Schunter, Christian Stüble und Michael Waidner. Besonderer Dank geht außerdem an unsere Kollegen vom ITAS, Knud Böhle, Carsten Orwat und Marcel Jakobsmeier, für die kritische Durchsicht und die konstruktiven Anmerkungen.

Glossar

Cloud Computing
Ein Teil der Hardware wie Rechenkapazität, Datenspeicher, Netzwerkkapazität oder auch Software wird auf Nutzerseite nicht mehr selbst betrieben oder örtlich bereitgestellt, sondern bei einem oder mehreren, meist geographisch entfernt liegenden Anbietern als Dienst gemietet. Die Anwendungen und Daten befinden sich dann nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der sogenannten „Wolke“ (engl. „cloud“). Durch die gemeinsame Nutzung von Ressourcen ergeben sich Kostenvorteile.

Collaborative Search Engines
Ein relativ neuer Ansatz sind Verteilte Suchmaschinen bzw. Föderierte Suchmaschinen. Dabei wird eine Suchanfrage an eine Vielzahl von einzelnen Computern weitergeleitet, die jeweils eine eigene Suchmaschine betreiben und die Ergebnisse zusammengeführt. Eine besondere Art sind die Collaborative Search Engines, die auf einem Rechner-Rechner-Verbindungsprinzip („Peer-to-Peer“) basieren. Jeder dieser Rechner kann Teile des Webs unabhängig erfassen, welche der jeweilige Nutzer durch einfache lokale Konfiguration definiert.

Datamining
Unter Datamining (dt. Datenschätze gewinnen) ist die systematische Anwendung von statistisch-mathematischen Methoden auf einen Datenbestand mit dem Ziel, Muster zu erkennen. Datamining wird vor allem bei manuell nicht mehr verarbeitbaren, also sehr großen Datenbeständen angewendet.

Datenschutz
Unter Datenschutz versteht man den Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten, oft auch im Zusammenhang mit dem Schutz der Privatsphäre. Zweck und Ziel ist die Sicherung des Grundrechts auf informationelle Selbstbestimmung der Einzelperson. Jeder Mensch sollte grundsätzlich selbst entscheiden, wem wann und welche Daten zugänglich sein sollen. Im englischen Sprachraum spricht man von „privacy“ (Schutz der Privatsphäre) und von „data privacy“ (Datenschutz im engeren Sinne).

Datensicherheit
Als Datensicherheit oder auch Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, welche die Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Datensicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen (wie z.B. Sabotage, Spionage oder Computerviren), der Vermeidung von Schäden und der Minimierung von Risiken.

Digitale Identität
Allgemein ist eine Identität eine eindeutige, wieder erkennbare Beschreibung einer natürlichen oder juristischen Person oder eines Objektes z.B. Personengruppe, Unternehmen, Rechner, Programm, Datei. In diesem Kontext ist eine digitale Identität eine Identität, die von einem Rechner verstanden und verarbeitet werden kann. Die digitale Identität entsteht, indem Attribute einer natürlichen Person oder eines Objektes in einem Rechner in elektronischer Form erfasst werden.

Informationelle Selbstbestimmung
Im bundesdeutschen Recht ist das Recht auf informationelle Selbstbestimmung das Recht des Einzelnen, grundsätzlich selbst, über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Dieses Datenschutz-Grundrecht wird im Grundgesetz für Deutschland nicht ausdrücklich erwähnt. Das Recht auf informationelle Selbstbestimmung ist weit gefasst. Es wird nicht unterschieden, ob mehr oder weniger sensible Daten des Einzelnen betroffen sind.

Location Based Services (LBS; Standortbasierte Dienste)
Dies sind mobile Dienste, die unter Zuhilfenahme von positionsabhängigen Daten dem Endbenutzer selektive Informationen bereitstellen oder Dienste anderer Art erbringen. Bei den LBS wird zwischen reaktiven und proaktiven standortbezogenen Diensten unterschieden. Bei reaktiven Diensten muss der gewünschte Service explizit angefordert werden, der proaktive Dienst wird z.B. beim Betreten einer bestimmten Zone automatisch aktiviert.

Mehrseitige Sicherheit
Mehrseitige Sicherheit bedeutet die Berücksichtigung der Sicherheitsanforderungen nicht nur einer der beteiligten Parteien. Speziell bei offenen Kommunikationssystemen vertrauen sich die Beteiligten per se nicht, sondern sind sämtlich als Angreifer zu verstehen. Aus diesem Grund sind die Anforderungen mehrseitiger Sicherheit bspw. bei für universelle Nutzung gedachten sozialen Netzwerken sehr anspruchsvoll. Anforderungen könnten sein: Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit.

Privatsphäre/ Privatheit
Privatsphäre bezeichnet den nicht-öffentlichen Bereich, in dem ein Mensch unbehelligt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt. Dieses Recht ist in allen modernen Demokratien verankert und gilt als Menschenrecht.

Personenbezogene Daten
Personenbezogene Daten sind gemäß §3 Abs. 1 Bundesdatenschutzgesetz (BDSG) „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. In Deutschland fallen nur die Daten einer natürlichen Person unter die gesetzliche Definition, während bspw. in Österreich, Luxemburg und Dänemark auch die Daten juristischer Personen in den Schutzbereich entsprechender Gesetze einbezogen sind. Beispiel für personenbezogene Daten: Augenfarbe, Geburtsort, Kontonummer, Matrikelnummer.

Zusammenfassung

Ende April 2011 haben zwei „Datenskandale“ für öffentliche Aufregung gesorgt. Zwei US-amerikanische Entwickler stellten ein Programm vor, mit dessen Hilfe von iPhone und iPad unverschlüsselt gespeicherte und mit dem PC synchronisierte Ortsdaten ein Bewegungsprofil der Nutzer erstellt werden kann. Nahezu zeitgleich musste der Elektronikkonzern Sony eingestehen, dass das Online-Netzwerk der Spielekonsole Playstation von Hackern angegriffen wurde und dabei sensible persönliche Daten von rund 80 Millionen Kunden entwendet wurden, darunter Kreditkarten-Datensätze.

Beide Fälle aus der jüngsten Vergangenheit sind Beispiele für durch moderne Informations- und Kommunikationstechnologien (IKT) hervorgerufene Problemstellungen, mit denen Technikentwickler, Unternehmen, Nutzer, aber auch Politik und Justiz umgehen müssen: Im Zuge des intensiven Austauschs von Informationen im **Web 2.0** und des Nutzens von **Lokalisierungsdiensten** und **Suchmaschinen** entstehen digitale Identitäten, die meist wissentlich und willentlich aufgebaut werden. Dennoch ist das Bewusstsein über den Verbleib der Daten und deren Weiterverwendung oftmals unzureichend, bis hin zum Problem unbewusster und nicht-intendierter Datenweitergabe und Datenmissbrauch z.B. von Daten, die Nutzer im Zusammenhang mit Telekommunikation und Transaktionen hinterlassen, die dann über Datamining u.a. zu personenbezogenen Daten hochgerechnet werden. Hinzu kommt, dass der Zugriff auf Daten im Netz kaum zeitlich begrenzt werden kann und die hinterlassene Datenspur fortbesteht. Wir sprechen deshalb in der vorliegenden Kurzstudie von ‚klebrigen’ Informationen.

Auch die **RFID-Technologie** und **Near Field Communication**-Szenarien berühren die Frage nach dem sicheren Umgang mit Informationen in einer digitalen Welt. Zunächst liegt deren Einsatzgebiet v.a. im Bereich der Handelslogistik, aber auch der öffentliche Sektor macht sich die Identifikation per Funk zunehmend zu Nutze, so z.B. im neuen ePersonalausweis. Vor allem das Problem, dass Daten möglicherweise von fremden Dritten ausgelesen und missbraucht werden können, spielt hierbei eine gewichtige Rolle. Eine Ausweitung der Nutzungsbereiche bis hin zur Personenüberwachung mittels RFID ist denkbar.

Digitale Identitäten und das Problem ‚klebriger’ Informationen sind eine Herausforderung für die Debatten um das Grundrecht selbstbestimmten Handelns und den Schutz der Privatsphäre. Es besteht die Schwierigkeit, dass aufgrund der ‚Klebrigkeit’ der Daten die Auswirkungen auf das Grundrecht zur Wahrung der Privatsphäre nicht mehr reversibel sind. Allerdings ist eine Diskrepanz auszumachen zwischen dem Wunsch nach Privatsphäre und dem „öffentlichen Verhalten“. Die Preisgabe privater Daten droht dabei – sofern sie überhaupt bewusst und intendiert erfolgt – mit dem Nutzen, der aus der Nutzung der modernen IKT resultiert, verrechnet zu werden.

Wie die Kurzstudie zeigt, beinhaltet das Phänomen ‚klebriger’ Informationen somit einige offene Fragestellungen und dringende Handlungsfelder für die Innovations- und Technikanalyse (ITA). Generell wäre eine Untersuchung zur Nutzung, Verkettbarkeit und Weiterverwendung von Daten bzw. Persönlichkeitsprofilen (Stichfragen: Wer? Was? Wie? Wo? Wann? Warum?) sinnvoll. Ein Ergebnis dieser Abwägung bzw. Analyse könnten u.a. verbindliche Regularien sein, die Missbrauch bestrafen und im besten Fall unterbinden.

Eine empirisch fundierte ITA sollte insbesondere die Diskrepanz zwischen von Experten konstatierten neuen Qualitäten potentieller Gefahren und dem faktischen Nutzerverhalten beleuchten und die Sicht der Konsumenten, aber auch Nutzer in Betrieben, stärker mit einbeziehen. Ausgehend von einer Analyse der bestehenden Kenntnisse der Nutzer über die mit der Datenweitergabe einhergehenden Risiken, soll Klarheit darüber hergestellt werden, wie sich die Einstellung der Nutzer zu Privatheit und informationeller Selbstbestimmung bei neuen Diensten und dem globalen Datenaustausch verhält und welche technischen und regu-

latorischen Maßnahmen zum Schutz der Privatsphäre auf Akzeptanz stoßen würden. Es gilt, konkrete Handlungsoptionen im technischen und rechtlichen Bereich zu eruieren, genauso wie einen Katalog von Maßnahmen zur Bewusstseinsbildung bei neuen Datendiensten zu erstellen, um die Schlüsse aus der Analyse des Nutzerverhaltens adäquat umzusetzen.

Verschiedene Ansätze technischer und juristischer Schutzmaßnahmen scheinen zum Ziel zu haben, den Daten- und Verbraucherschutz im Bereich digitaler Identitäten zu stärken. Privacy Enhancing Technologies (PET) stehen für Programmfunktionen und Tools, die technische Möglichkeiten des Datenschutzes bieten, v.a. Anonymisierung, Unverkettbarkeit von Daten und Managementtools für persönliche Daten. Einer grundsätzlichen Klärung sollte jedoch auch die Frage potentieller Sicherheitslücken von Endgeräten zugeführt werden, da über diese, die Sicherheitseinstellungen vorgenommen und kontrolliert werden.

Nach den Vorkommnissen der letzten Monate in der arabischen Welt bekommt die Diskussion um das politische Potential von Facebook etc. und der Welt der digitalen Kommunikation insgesamt Auftrieb. Welche Rolle die Möglichkeit sicherer und anonymer globaler Kommunikation für Demokratisierungsprozesse spielt und welche Chancen und Risiken insgesamt damit einhergehen, könnte parallel analysiert werden.

Wie die Kurzstudie insgesamt zeigt, sind Fragen zum Datenschutz, zur Privatsphäre und informationeller Selbstbestimmung in der digitalen Welt bereits in zahlreichen (ITA)-Studien Untersuchungsgegenstand und somit als Thema in der ITA angekommen. Für einige, in der vorliegenden Studie angesprochenen Anwendungsmöglichkeiten moderner IKT mangelt es jedoch derzeit noch an Vorschlägen zur Umsetzung konkreter technischer und juristischer Handlungsoptionen. Diese wären bspw. durch spezielle ITA-Studien noch systematisch zu untersuchen. Generell erhebt die vorliegende Kurzstudie potentielle Folgen im Umgang mit klebriger Information und identifiziert aus den skizzierten Problemfeldern Themen für eine zukünftige ITA-Forschung.

1 Einführung in das Thema

«The digital revolution has changed everything...
What was once hard to copy is now trivial to duplicate.
What was once forgotten is now stored forever.
What was once private is now public.»
Ronald L. Rivest (2001)[1]

Heutzutage erlauben moderne Informations- und Kommunikationstechnologien Individuen einen unkomplizierten Austausch von Informationen und machen diese Informationen in einem bisher unbekannten Ausmaß öffentlich und global verfügbar. Soziale Medien wie z.B. Facebook, MySpace, Twitter und StudiVZ mit über 1 Milliarde Mitgliedern[2] auf der ganzen Welt, sind dabei zwar das seit Anfang 2010 in der Öffentlichkeit wie auf wissenschaftlicher Ebene[3] am stärksten diskutierte, aber nicht das einzige Beispiel dieses Phänomens. Auch durch Personensuchmaschinen, wie beispielsweise der Google-Dienst 23andme.com[4], der anbietet, den persönlich bereitgestellten DNA-Code nach Verwandschaftsverhältnissen rund um die ganze Welt zu untersuchen, die Aufzeichnung von Recherchegewohnheiten bei der Nutzung von Suchmaschinen oder durch Lokalisierungsdienste, entstehen digitale Identitäten[5]. Daneben nutzen auch öffentliche Stellen immer mehr persönliche Daten für verschiedenste Zwecke, wie z.B. die Verfolgung von Individuen im Falle des Ausbruchs einer Epidemie, um Terrorismus und Kriminalität effektiver zu bekämpfen und zu verhindern, zur Gewährleistung der sozialen Sicherheit und für steuerliche Zwecke als Teil von eGovernment (Euro 2010). Zur selben Zeit werden die Wege der Datensammlung elaboriert und aufgrund der Vielzahl weltweit und dezentral verteilter Akteure undurchsichtiger. Profile und Identitäten werden somit einerseits wissentlich und willentlich aufgebaut und weiterentwickelt, andererseits scheint es nach Aussagen einiger Experten den Nutzern z.B. im Zusammenhang mit Telekommunikation und Transaktionen häufig gar nicht oder nur unzureichend bewusst zu sein, dass durch Datamining u.a. sensible personenbezogene Daten generiert und gespeichert werden. Außerdem haben auch Hackerangriffe auf Unternehmen die Aufmerksamkeit der breiten Öffentlichkeit erreigt, wie beispielsweise der Elektronikkonzern, der eingestehen musste, dass das Online-Netzwerk der Spielekonsole Playstation angegriffen wurde und dabei sensible persönliche Daten von rund 80 Millionen Kunden entwendet wurden, darunter Kreditkarten-Datensätze (von Streit 2011).

Datenschützer, Technikexperten, Unternehmen, Nutzer, aber auch Politik und Justiz sowie Technikfolgenabschätzer sehen potentiell neue Gefahren für den Datenschutz und die informationelle Selbstbestimmung insbesondere darin, dass einmal digital erfasste personenbezogene Daten auch nach Jahren noch zugreifbar und auswertbar bleiben. Man kann sich somit nicht mehr von seiner Internet-Identität lösen, so dass wir von einm ‚Kleben' der Informationen der Nutzer sprechen. Bisher bleiben auch nach dem Löschen durch den Nutzer alle Daten und Einträge noch jahrzehntelang im Netz abrufbar, da den Nutzern die technischen und rechtlichen Grundlagen fehlen, diese Profile aus dem Internetgedächtnis löschen zu können (Mayer-Schönberger 2008).

Neben der langen Verfügbarkeit von personenbezogenen Daten im Netz können durch immer leistungsfähigere Speichermedien und Prozessoren Daten mit immer effizienteren Algorithmen automatisiert zu fein-

---

1 Ronald L. Rivest. Whither information security? http://wean1.ulib.org/Lectures/DistinguishedLectures/2001/03.0RonaldLRivest/, Invited talk at the SCS Distinguished Lecture Series. März 2001

2 Mitgliederzahl zitiert nach (Rudlstorfer 2010).

3 U.a. sprachen die Experten des im Rahmen des Projekts durchgeführten Workshops dem Thema eine hohe Relevanz zu und wiesen auf die Dringlichkeit der Problematik hin.

4 www.23andme.com

5 Vgl. unter anderem (Heatherly, 2009).

granularen Interessens-, Konsum- und Bewegungsprofilen[6] von Personen verkettet und ausgewertet werden. Das Verkleben bzw. die Verkettung von Daten und das Handeln mit daraus resultierenden Persönlichkeitsprofilen geben der schon länger andauernden Diskussion zu Datenschutz und Privatsphäre eine andere Qualität und stellen den Staat, Datenschützer und Andere vor neue Herausforderungen. Die Problematik durch den Kontextverlust, der mit einer Daten- oder Techniknutzung in ganz anderen als den für die Entstehung implizierten Zusammenhängen verbunden ist, wird nach Aussagen von seriösen Forschern sogar noch verschärft. Beispielsweise könnten RFID-Chips oder Technologien wie das Global Positioning System (GPS) anstatt den Standort eines Produktes in Lieferketten zu lokalisieren, zur Verfolgung und Überwachung von Menschen genutzt werden.

Aufgrund der Komplexität des Themas werden im Folgenden die interdependenten Beziehungen von Technologien und Gesellschaft auf Fragestellungen zum Umgang mit personenbezogenen Daten im Internet fokussiert. Auf verwandte Aspekte bei der Datenerhebung und -speicherung, wie z.B. bei Scoring-Systemen der Finanzindustrie (Schufa, easycash etc.) oder bei Unternehmen wie payback o.a., wird in der vorliegenden Studie nicht eingegangen. Aufgrund der Relevanz werden derartige Fragestellungen aber im Rahmen des Projektes in gesonderten Analysen wie „IKT im Finanzsektor“ untersucht.

Vor dem Hintergrund der Zielstellung ist der Aufbau der Studie wie folgt angelegt:

In Kapitel 2 wird der Stand der Forschung und Entwicklung problembezogen diskutiert, und das sowohl bezogen auf die technischen Grundlagen als auch entlang der oben beschriebenen ITA-Dimensionen. Dabei sollen einige zentrale Aspekte der verschiedenen Technikkonzepte wie z.B. Location Based Services (LBS; Standortbasierte Dienste) angesprochen werden. Hierbei geht es vor allem um eine prägnante Darstellung potentieller Folgen aktueller und zukünftiger IT-Szenarien, wie sie in ITA- und Fachkreisen diskutiert werden, also z.B. von Fachleuten aus Ministerien und Parlamenten, Datenschutzorganisationen, Forschern, Marktanalysten und Unternehmen. Darauf aufbauend erfolgt in Kapitel 3 die Darstellung offener Fragestellungen, die bspw. durch spezielle ITA-Studien noch systematisch zu untersuchen wären. Kapitel 4 zeigt Vorschläge zur methodischen Umsetzung auf, die sich durch die bisher ungeklärten Fragestellungen aus dem vorhergehenden Kapitel ergeben.

In dieser Studie wurde durchgängig das Maskulinum in seiner generischen Funktion verwendet. Auf ein Gendering wurde zugunsten der Lesbarkeit verzichtet.

[6] Zwei US-amerikanische Entwickler stellten ein Programm vor, mit dessen Hilfe von iPhone und iPad unverschlüsselt gespeicherte und mit dem PC synchronisierte Ortsdaten ein Bewegungsprofil der Nutzer erstellt werden kann (Lischka, Reißmann, Kremp 2011).

2 Status Quo von Forschung und Entwicklung

2.1 Technologische Konzepte

In den nachfolgenden Kapiteln werden kurz die Charakteristiken sowie die derzeitigen und zukünftigen Anwendungsgebiete unterschiedlicher technologischer Konzepte wie z.B. Web 2.0-Dienste dargestellt. Auf eine ausführliche Darstellung der möglichen nicht-intendierten Konsequenzen wird in diesem Kapitel verzichtet. Sie erfolgt im Kapitel 2.2 „Folgedimensionen".

2.1.1 Vision einer allgegenwärtigen Datenverarbeitung

Aufgrund ihrer minimalen Größe und ihres geringen Preises und Energiebedarfs können Prozessoren mit integrierter drahtloser Kommunikationsfähigkeit und Sensoren bald in vielen Alltagsgegenständen integriert oder anderweitig in die Umwelt eingebracht werden. Selbst Dinge, die primär keine elektrischen Geräte darstellen, werden dadurch in die Lage versetzt Informationen zu verarbeiten und (miteinander) zu kommunizieren („**Internet der Dinge**"). In Kombination mit den oben skizzierten Kommunikations- und Lokalisierungstechnologien ist nach Adamowsky (2010) damit die Voraussetzung für eine total vernetzte, informatisierte Welt, dem sog. **Ubiquitous Computing**[7] geschaffen. Der Begriff Ubiquitous Computing wurde bereits 1991 von Mark Weiser (1991) geprägt:

> *"Most of the computers that participate […] will be invisible in fact as well as in metaphor. […] These machines and more will be interconnected in a ubiquitous network."*

Der PC ist in der Betrachtungsweise von Experten in dieser Vision nur ein Zwischenschritt zu allgegenwärtig, unsichtbar integrierten Technologien, die permanent miteinander kommunizieren, Daten speichern können und dabei den Menschen bei einer beträchtlichen Anzahl seiner Tätigkeiten und bei der Selbstversorgung und unabhängigen Lebensführung unmerklich unterstützen (Dritsas, Tsaparas, Gritzalis 2006; Orwat et al. 2008)[8]. Dies würde Alltagsgegenständen eine neue, zusätzliche Qualität verleihen. Sie könnten orten, wo sie sich befinden, welche Gegenstände oder Personen in der Nähe sind, sie hätten eine Art ‚Gedächtnis' und eine gespeicherte Vergangenheit. Das allgegenwärtige Computing könnte sämtliche Lebens- und Wirtschaftsbereiche durchdringen und zum Beispiel den privaten Komfort in der Wohnung oder dem Haus erhöhen („intelligentes Haus" oder „Ambient Assisted Living"[9]). „Intelligente Fahrzeuge" würden Verkehrswege sicherer machen und implantierte Sensoren und Kleinstcomputer könnten den Gesundheitszustand des Nutzers überwachen. Einige Experten vertreten die Ansicht, dass sich daneben grundsätzlich Möglichkeiten bieten würden, betriebliche und überbetriebliche Prozesse effizienter zu gestalten, sowie neue Produkte und Dienste zu entwickeln.

Als Teilgebiete des Ubiquitous Computing können aufgrund der Mobilität der Dinge als eine Grundvoraussetzung für die Visionen der Allgegenwärtigkeit auch das **Mobile Computing** (s. Kapitel 2.1.3 Kommunikationstechnik), Entwicklungen im Bereich von „**Drahtlosen Sensornetzen (Smart Dust)**[10]" und **(Wirel-**

---

[7] Ubiquitous Computing wird auch als Ubicomp, Pervasive Computing, Ambient Intelligence, Smart Dust, Nomadic Computing und als Internet der Dinge bezeichnet. Der begriffliche Unterschied ist dabei eher akademischer Natur. Gemeinsam ist allen das Ziel den Menschen zu unterstützen sowie wirtschaftliche wie soziale Prozesse durch eine Vielzahl von in die Umgebung eingebrachten Mikroprozessoren und Sensoren zu optimieren.

[8] Vgl. dazu auch Szenarien in (Bizer et al. 2006) und (Friedewald et al. 2009b).

[9] Vgl. dazu das Förderprogramm des BMBF „Assistenzsysteme im Dienste des älteren Menschen", Informationen unter http://www.aal-deutschland.de und z.B. (Gaßner, Conrad 2010).

[10] Smart Dust (oder „Intelligenter Staub") wird in dieser Studie nicht näher betrachtet, da im Rahmenprogramm Mikrosysteme 2004-2009 ("Mikrosystemtechnik für autonome vernetzte Sensorsysteme") sowie im Förderungs-

ess) Body Area Networks ((W)BAN), angesehen werden. Mit (W)BANs ist eine (drahtlose) Anbindung von am Körper getragenen medizinischen Sensoren und Aktoren möglich. Durch das Anfassen eines Gegenstandes oder Gerätes übermittelt z.B. die Armbanduhr eine eindeutige Personen-Identifikation und ermöglicht so den Zugang zu einem bestimmten System (von PC-System bis zu einem Konzert). Ebenso können Körperfunktionen, wie z.B. Blutdruck und Puls erfasst werden, die zur medizinischen Diagnose dienen, sowie biometrische Daten und Implantate überwacht werden. Somit wird nach Meinung von Heesen und Simoneit (2007) auch der Körper eines Individuums zu einem Teil des Datentransfers.

Eine Weiterentwicklung der WBANs stellen tragbare Computersysteme (**Wearable Computing, Wearables**) dar. Bei den tragbaren Computersystemen handelt es sich um in die Kleidung („i-Wear" oder „intelligente Kleidung") integrierte oder am Körper getragene miniaturisierte elektronische Geräte. Die Besonderheit hierbei ist, dass die originäre Tätigkeit des Benutzers nicht die Benutzung des Computers, sondern eine durch den Computer unterstützte Tätigkeit und eine handfreie Interaktion, Multifunktionalität und Kontextsensitivität umsetzbar ist. Das Funktionsspektrum der Wearables umfasst die Erfassung und Verarbeitung von Körper- und Umgebungsdaten sowie die Kommunikation über das Internet oder lokale Netze. Beispiele für Wearables sind Armbanduhren, die ständig den Puls messen[11], Brillen, deren Innenseiten als Bildschirm dienen oder Kleidungsstücke, in die elektronische Hilfsmittel zur Kommunikation und Musikwiedergabe oder Sensoren[12] eingearbeitet sind, bis hin zu Videos in Brillen.

In allen diesen Teilgebieten des Ubiquitous Computing werden sensible (personenbezogene) Daten generiert, so dass auch nicht-intendierte Nebenfolgen in Betracht gezogen werden müssen, speziell in Anbetracht der informationellen Selbstbestimmung und des Schutzes der Privatsphäre. Einen umfassenden Überblick u.a. über verschiedene Szenarien der Unsicherheit von Systemen des Ubiquitous Computing und mögliche Lösungsstrategien bietet (Gabriel 2006).

2.1.2 Web 2.0[13]-Dienste

Die technologischen Entwicklungen interaktiver und kollaborativer Dienste des Web 2.0 der letzten Jahre machen es möglich, viele Arten menschlicher sozialer Kontakte in Netzwerken, wie Facebook[14], StudiVZ[15], Friendsticker[16], Xing[17] etc. oder Diensten wie Twitter[18], digital abzubilden. Dank derartiger Dienste können Personen Kontakt miteinander aufnehmen und aufrecht erhalten, der sonst aufgrund räumlicher oder anderer Barrieren schwer oder unmöglich wäre. Auf diese Weise finden aber nicht nur ‚Freunde' zu-

programm "IT-Forschung 2006" (Forschungsbereich "Kommunikationstechnologien") das BMBF die Entwicklung von innovativen Lösungen in diesem Bereich bereits mit mehr als 15 Millionen Euro gefördert hat und dabei auch Ansätze zur Sicherung der Privatsphäre und zur Erhöhung der Datensicherheit untersucht wurden.

11 Im Aachener European Microsoft Innovation Center (EMIC)-Labor wird z.B. eine „SPOT Watch" entwickelt, die bei der Überwachung von Diabetikern eingesetzt werden soll. Die Uhr soll Daten von einem mit einem Sensor ausgestatteten T-Shirt erhalten und dann Vorschläge für die nächste Insulin-Dosierung machen (http://www.microsoft.com/emic).

12 Das europaweite Konsortium wearIT@work, entwickelt für den Einsatz bei der Feuerwehr Sensoren, die in die Kleidung integriert werden und Vitaldaten usw. messen. Ein weiteres Beispiel ist senSAVE, ein Gemeinschaftsprojekt von fünf Fraunhofer-Instituten. Hier sollen funkvernetzte Sensoren im Hemd den Gesundheitszustand überwachen. Ein speziell ausgestattetes Smartphone speichert und analysiert die Daten und ruft im Notfall automatisch den Arzt an. Für weitere Informationen: http://www.wearitatwork.com/ und http://www.fit.fraunhofer.de/projects/mobiles-wissen/sensave.html.

13 Der Begriff Web 2.0 wird für eine Reihe interaktiver und kollaborativer Dienste des Internets verwendet. Die Versionsnummer 2.0 postuliert eine neue Generation des Webs. Näheres unter http://www.web2summit.com/web2009/public/schedule/detail/10194

14 www.facebook.com

15 www.studivz.net

16 www.friendsticker.com

17 www.xing.com

18 www.twitter.com

sammen, sondern alle Personen mit gleichen Interessen, Arbeits- oder Themengebieten können, in welcher Form auch immer, miteinander kommunizieren und zusammenarbeiten. Nicht zuletzt durch das Web 2.0 haben sich neue Formen der Informations- und Kommunikationstechnologien zur Unterstützung von sozialen Interaktionen und kollaborativer Arbeit entwickelt („collaborative working"): **Social-Networking-Services** (SNS) oder **Mobile Social Network** (MSN). SNS bezeichnen Anwendungssysteme, die nach Richter und Koch (2008) sechs Funktionalitätsgruppen kombinieren:

> *„Identitätsmanagement, (Experten-)Suche, Kontextawareness (Kontext/ Vertrauensaufbau), Kontaktmanagement, Netzwerkawareness und gemeinsamer Austausch (Kommunikation)."*

Eine Besonderheit der Web-2.0-Anwendungen ist, dass die Nutzer zwischen der Rolle des Dienstnehmers sowie des Dienstgebers wechseln.

Eine weitere Web 2.0-Anwendung stellen (Meta-)Suchmaschinen oder auch sog. **Collaborative Search Engines** (CSE) wie z.B. Yet another Cyberspace[19] (YaCy) dar.

2.1.3 Kommunikationstechnik

Neben technischen Fortschritten mit einem Trend zu immer höheren Datenraten ist vor allem die drahtlose Kommunikation (**Mobile Computing**) für die Informatisierung des Alltags und den unmittelbaren persönlichen Zugang zu Informationen relevant. So sind Smartphones, Note- und Netbooks, multifunktionale Tablett-PCs, Handheld-PCs[20] und ein drahtloser Internetzugang per WLAN bereits Standard; und immer neuere Technologien ermöglichen eine noch schnellere Datenübertragung bei gleichzeitig fortschreitender Miniaturisierung und geringerem spezifischem Energiebedarf. Durch die mobile Verfügbarkeit des Internets bieten sich vielfältige Möglichkeiten, objekt- oder standortbezogene Informationen jederzeit direkt vor Ort bereit zu stellen und nicht nur ‚statisch' am heimischen PC abzurufen. Neben klassischen Webseiten können nun auch multimediale Inhalte wie Filme und Audiospots mit realen Objekten verknüpft werden. Bereits verfügbare Technologien für mobile Informationssysteme sind beispielsweise Quick-Response (QR)-Codes und Bluetooth-Systeme, die seit einigen Jahren von verschiedenen Unternehmen als Instrument des mobilen Marketings genutzt werden (vgl. dazu Beispiele in Steimel, Paulke, Klemann 2008; Weber 2007).

Interessant in diesem Zusammenhang sind u.a. **Radio Frequency Identification** (RFID)**-Systeme**, die eine Fernidentifikation per Funk ermöglichen. Bestehend aus einem RFID-Tag (Transponder[21]) mit einer eindeutigen Identifikationsnummer (ID) und einem Scanner/ Lesegerät können die Daten ohne Sichtkontakt oder Berührung ausgelesen werden. Der RFID-Tag kann aufgrund seiner minimalen Größe und seines relativ geringen Preises auf allen Arten von Gegenständen angebracht und Menschen[22] (Arte 2008) und Tieren implantiert werden, Objekte kennzeichnen sowie eine Vielzahl an Information über Art, Verwendungszweck, Standort, Herstellungsdatum etc. und sogar personenbezogene Daten[23] liefern. Damit kann ein

---

19 http://yacy.net/index_de.html

20 Z.B. von Acer, Casio, Hewlett Packard, IBM, Samsung, Sharp, Sony.

21 Ein Transponder ist ein mikroelektronischer Schaltkreis, bestehend aus einer Sende- und Empfangsantenne, einer Steuerlogistik und einem Datenspeicher. Solche Transponder, die sich z.B. für das Aufkleben oder Einlaminieren eignen sind nur 300-400 µm dünn.

22 In Mexiko tragen mehr als 1000 Menschen solche Chips, hauptsächlich aus medizinischen Gründen (Notarzt hat bei einem Unfall alle Informationen über den Patienten), aber auch bei ‚entführbaren' Menschen wird vor allem in Südamerika die RFID-Technik zur Ortung eingesetzt.

23 Dieser Mikrochip wird beispielsweise den Gästen einer Diskothek in Barcelona unter die Haut implantiert und dient zur Identifikation sowie zur Bezahlung: „We are the first discotheque in the world to offer VIP VeriChip. Using an integrated (imbedded) microchip, our VIPs can identify themselves and pay for their food and drinks without the need for any kind of document". (http://www.bajabeach.es/)

‚Tracking und Tracing' von Gütern, Tieren und Personen realisiert werden (vgl. u.a. van't Hof, Cornelissen 2006).

Vorangetrieben wird die RFID-Technik nach Aussagen von Friedewald und Lindner (2009a) vor allem von Anwendungsmöglichkeiten im Bereich der Logistik[24]: In der informatorischen Erfassung und Optimierung der Liefer- und Wertschöpfungskette liegt viel Rationalisierungspotential um Vorgänge transparenter, effizienter (Al-Kassab 2010) und besser aufeinander abgestimmt durchführen zu können (Schmitt, Thiesse, Fleisch 2007). Die Just-in-Time- oder die Just-in-Sequence-Produktion kann durch das automatisierte Preisgeben von Produktidentitäten weiter ausgebaut, Lagerhaltung weiter minimiert und Kosten gesenkt werden. Laut der TAUCIS-Studie „Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung" könnte daneben eine Dokumentation und Erfassung relevanter Transportparameter (z.B. Temperatur) durch die Kombination von RFID-Technik und entsprechender Sensorik realisierbar sein (Bizer 2006). Nach dem Omnicard Newsletter wird jedoch 2010 immer noch getestet, wie RFID-Tags identifiziert werden können, wenn sie dicht gepackt sind, wie bei CDs oder auf metallischen Waren angebracht (Omni 2010).

Realität ist die RFID-Technologie im neuen ePass. Seit dem 1. November 2007 sind bei der 2. Generation der ePässe neben dem Foto auf dem Funkchip Abdruckbilder von zwei Fingern gespeichert (BMI 2010a). Ab November 2010 wird der neue ePersonalausweis den bisherigen Personalausweis ablösen (BMI 2010b)[25].

Zukünftig könnte man zudem als Kunde, ähnlich wie bei dem von der Metro Group bereits im April 2003 eröffneten Future Store[26], den am Einkaufswagen befindlichen sog. Personal Shopping Assistent (PSA) nutzen. Der PSA könnte neben dem Bereitstellen von individuell gewünschten Produktinformationen auch Supermarktkassen obsolet werden lassen, da die am PSA eingelesenen Daten direkt an die Kasse übertragen werden und zukünftig ohne Kontakt zum Ladenpersonal per EC- oder Kreditkarte bezahlt werden könnte. Das Konzept „Metro Group Future Store" wurde u.a. von der European Technology Assessment Group des Europäischen Parlaments untersucht (van't Hof 2007).

Da über die eindeutige ID von RFID-Tags, Objekte in Echtzeit mit einem im Internet befindlichen oder einer standortunabhängigen Datenbank zugehörigen Datensatz verknüpft werden können, kann diesen Dingen eine spezifische Information zugeordnet werden. Der so mögliche flexible Informationszugewinn des einzelnen Gegenstands eröffnet in Zukunft aber weit über den intendierten Zweck der automatisierten Lagerhaltung, des kassenlosen Supermarktes oder des selbstständigen Einkaufs des interaktiven Kühlschranks (siehe „Internet der Dinge") hinausgehende Anwendungsmöglichkeiten. Ob solche Dinge wirklich realisiert und nachgefragt werden, lässt sich allerdings schwer vorhersagen. Da jedoch eine weitere Miniaturisierung und Kostenreduzierung zu erwarten ist, kann nach einer Studie des Büros für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) davon ausgegangen werden, dass RFID-Technologien entsprechend ihres Charakters als typische Querschnittstechnologie in den Bereichen Wohnen, Arbeit und Wirtschaft, Freizeit, Einkauf, Reisen und Verkehr sowie dem Gesundheitswesen neben den aktuellen noch bei weiteren Anwendungen zum Einsatz kommen könnten (Friedewald et al. 2009a). Hindernisse könnten Datenschutzaspekte sowie Fragen der Sicherheit (siehe z.B. Oertel et al. 2004) und der Strahlenbelastung

[24] Eins der wenigen Vorreiterunternehmen bei RFID-Pilotanwendungen in Deutschland ist die DHL International GmbH, ein Tochterunternehmen der Post, die seit 2006 das „DHL Innovation Centre" betreibt. In diesem sollen RFID-Trends in marktfähige Produkte umgewandelt werden (http://www.dhl-innovation.de/).

[25] „Die neue Dokumentengeneration wird die herkömmlichen Anwendungen des Ausweises um elektronische Funktionen ergänzen. Die Daten, die heute optisch vom Dokument ablesbar sind, werden zukünftig in einem Ausweis-Chip abgelegt. Damit können sich die Ausweisinhaber online ausweisen – sowohl gegenüber Behörden im E-Government als auch gegenüber privatwirtschaftlichen Dienstleistungsanbietern beispielsweise bei Online-Shopping, Online-Banking oder beim Online-Kauf von Tickets." (BMI 2010)

[26] http://www.future-store.org/; abgerufen am 21.06.2010

sowie die bisher wenigen Anwendungslösungen sein, die z.B. in einer Studie vom Institute for Prospective Technological Studies für die EU-Kommission adressiert wurden (van Lieshout, Kool 2007) und in Kapitel 2.2 „Folgedimensionen“ dargestellt werden.

Ein Kommunikationsprinzip, das ähnlich zur RFID funktioniert, allerdings nur über Distanzen von wenigen Zentimetern, ist die sog. **Near Field Communication** (NFC), die u.a. durch das Center for Near Field Communication der Universität Hannover untersucht wurde (Wiedmann, Reeh, Schumacher 2010). NFC ist für die Übertragung kleiner Datenmengen in einem nahen Umfeld von wenigen Zentimetern konzipiert. Da für die Kommunikation physische Nähe[27] zwischen Tag und Scanner erforderlich ist, wird die NFC-Technologie vor allem für bargeldlose Bezahlungen, Ticketing, Unterhaltungen und Zugangskontrollen eingesetzt. Aufgrund der geringen Größe von NFC-Einheiten können diese leicht in Mobiltelefone integriert werden. Nach Aussagen von manchen Experten und von Unternehmern[28] sollen Mobiltelefone zunehmend mit NFC-Lesegerät ausgestattet werden (EPoS 2008; Reynolds 2008; Vanjoki 2010). Das Handy kann dann die empfangenen Daten entweder direkt interpretieren und anzeigen oder weitere Informationen über das Mobilfunknetz anfordern bzw. mit einem Server im Internet agieren, dessen Internetadresse auf dem Transponder gespeichert ist. Dadurch wären etwa Szenarien denkbar, wo z.B. Touristen mit Points-of-Interest interagieren[29] und dabei Videoclips zugespielt bekommt oder Kunden Konzertkarten reservieren und zeitgleich einen Musikclip auf das Handy geladen bekommen. Die Deutsche Bahn nutzt NFC-Technologien in ihrem Pilotprojekt „Touch & Travel“[30], das seit 2008 mit einigen Testkunden auf Strecken zwischen Berlin, Hannover, Frankfurt und dem Ruhrgebiet durchgeführt wird. Hierbei handelt es sich um ein neues e-Ticketing-Verfahren, bei dem Bahnkunden zukünftig durch An- und Abmelden an sog. Touchpoints Fahrkarten mobil kaufen und abrechnen können. In der Stadt Hanau bei Frankfurt wurde NFC nach Aussagen der Deutschen Bahn zwar bereits in den Regelbetrieb für den öffentlichen Nachverkehr als Handy-Ticketing-System übernommen, der Einsatz im Betrieb scheiterte aber bisher an der geringen Verfügbarkeit von NFC-Handys. Trotz dieser NFC-Anwendungen im eTicketing haben sich bislang in Deutschland die Technologien aber wegen des abwartenden Verhaltens der Industrie noch nicht gegen Technologien wie Bluetooth flächendeckend durchsetzen können (Madlmeyer et al. 2008). In Hongkong und Japan hingegen weisen NFC-Technologien vor allem für Bezahldienste schon seit 2001 eine hohe Marktpenetration auf (Weber 2001; KPMG 2009).

2.1.4 Lokalisierung

Zur Lokalisierung von mobilen Objekten, Tieren und Personen existieren bereits verschiedene technische Ansätze. Neben der bereits beschriebenen Lokalisierung über **RFID-Tags** oder **NFC** bzw. über Funkzellen von Sendern, deren Positionen bekannt sind und deren Genauigkeit nicht besonders hoch ist, stellt die Entfernungsbestimmung via Laufzeitmessung von Funksignalen eine präzisere, jedoch auch aufwändigere Methode dar. Ein bekanntes System ist das satellitenbasierte **Global Positioning System** (GPS); der Endausbau des ähnlich konzipierten, originär zivilen europäischen Galileo-Systems soll bis Ende 2013 erfolgen. Einschränkend ist die Tatsache, dass diese Systeme bisher nur bei ‚Sichtkontakt’ zu den Satelliten funktionieren. Dennoch sind viele Handys mit GPS-Empfängern ausgestattet.

---

[27] Das Prinzip der physischen Annäherung ist der menschlichen Kommunikation nachempfunden.

[28] “All new Nokia Smartphone to come with NFC from 2011, A. Vanjoki, Nokia's executive vice president for markets, has announced that all new Smartphone introduced by the company from 2011 will come with NFC”, 17. June 2010 unter http://www.cnm.uni-hannover.de, NFC-Newsticker, aufgerufen am 21.06.2010.

[29] 2006 wurde auf der Nordseeinsel Sylt ein solches Informationssystem mittels NFC-Technologie aufgebaut. An bestimmten Punkten wie Restaurants oder Bushaltestellen wurde ein Transponder angebracht und der Nutzer konnte sich vor Ort informieren. Das System konnte sich allerdings nicht richtig durchsetzen, da es lediglich mit einem Handymodell funktionierte, das auf der Insel ausgeliehen werden musste.

[30] www.touchandtravel.de

Zur Handyortung wird derzeit ebenso das in vielen Ländern flächendeckende Mobilfunknetz **Global System for Mobile Communications** (GSM) verwendet. GSM-Ortung stellt, je nach Anwendungsfall, eine einfache Alternative zum GPS dar, da für das Mobilgerät keine weitere Infrastruktur benötigt wird. Die GSM-Ortung ist jedoch im Vergleich zur Standortbestimmung mittels GPS ungenauer, denn die zur Standortbestimmung herangezogenen Signale weisen systembedingte Toleranzen auf. Bei dem Mobilfunksystem **Universal Mobile Telecommunications System** (UMTS) der dritten Mobilfunk-Generation ist aus technischer Sicht eine bis zu 10 mal genauere Lokalisierung im Vergleich zu GSM möglich. Eine weitere Lokalisierungsmöglichkeit beruht auf **Wireless Local Area Network** (WLAN)-Zugangspunkten, die auch innerhalb von Gebäuden ortbar sind und städtische Bereiche weitgehend abdecken. Im Jahr 2010 geriet Google in die Diskussion, weil beim Fotografieren von Straßen für „Street View" auch WLAN-Daten aufgezeichnet wurden (Schubert 2010). Daneben scheint das iPhone von Apple zahlreiche Verbindungsdaten zurück zum Hersteller zu übermitteln (SpOn 2010).

Alle diese Technologien ermöglichen standortbezogene Dienste (**Location Based Services**; LBS). Dies sind mobile Dienste, die unter Zuhilfenahme von positionsabhängigen Daten dem Endbenutzer selektive Informationen bereitstellen oder Dienste anderer Art erbringen. Bei den LBS wird zwischen reaktiven und proaktiven standortbezogenen Diensten unterschieden. Bei reaktiven Diensten muss der gewünschte Service explizit angefordert werden, der proaktive Dienst wird z.B. beim Betreten einer bestimmten Zone automatisch aktiviert. Durch einen zusätzlich im Mobiltelefon eingebauten digitalen Kompass wird es möglich, die Blickrichtung des Nutzers festzustellen, wie in Japan seit 2007 im Einsatz (Billich 2007). Mit diesen Bezugspunkten ist es möglich, Informationen zum gerade anvisierten Objekt in Echtzeit im Handydisplay darzustellen. Diese ortsbezogenen Anwendungen (mobile Applications; Apps) sind u.a. für Unternehmen interessant, da sie ihnen erlauben, Verbraucher zu Filialen oder Restaurants in der Nähe zu lenken und diese gleichzeitig über ihr Produktangebot zu informieren und ihnen beispielsweise Gutscheine zu übersenden. Dieses so genannnte Location Based Advertising (LBA) wurde u.a. in dem Forschungsprojekt „E-LBA" der Europäischen Union untersucht.[31] Auch die kollaborativen Netzwerke wie Twitter, Facebook oder Foursquare[32] bieten mittlerweile Dienste an, bei denen sich die Nutzer an ihrem aktuellen Standort, wie z.B. einem Restaurant „anmelden" können. Der Standort wird dann für die Netzwerk-„Freunde" auf einer Karte sichtbar.

2.1.5 Technologien und Konzepte zum Schutz der Privatsphäre

Unter dem Oberbegriff Privacy Enhancing Technologies (PET) werden Technologien und Konzepte zur Herstellung von Anonymität und Unverkettbarkeit sowie auch zum Management persönlicher Daten verstanden:

> *[...] an umbrella term for schemes providing various levels of anonymity and unlinkability."* (Hyppönen, Hassinen, Trichina 2008)

beziehungsweise

> *"Privacy Enhancing Technologies (PET) are the technical answer to social and legal requirements. PET become constituent for tools to manage users' personal data. Users can thereby control their individual digital identity, i.e. their individual partial identities in an online world."* (Hansen, Meissner 2004)

[31] http://www.e-lba.com/

[32] Das kann skurrile Formen annehmen: 2010 reiste ein Schüler des Elite-Internats Eton, per Helikopter an den Nordpol, um bei Foursquare das „Last-Degree"-Abzeichen zu ergattern, für den ersten Eintrag am nördlichsten Breitengrad. Es ist bis jetzt seine einzige Aktion in diesem Netzwerk geblieben. Es ging lediglich ‚um die Ehre'.

Als Grundsätze für die datenschutzfördernde Technikgestaltung können nach Hennig et al. (2004) und Sieker et al. (2005) u.a. folgende Gesichtspunkte betrachtet werden:

- Transparenz,
- Anonymisierung und Pseudonymisierung bis hin zur Unverkettbarkeit (Chaum 1992; Pfitzmann, Pfitzmann, Waidner 1988),
- Datenvermeidung und Datensparsamkeit, d.h. keine zentralen Datenbanken,
- Verschlüsselung
- Systemdatenschutz, d.h. insbesondere technisch eingebauter Datenschutz,
- Selbstdatenschutz, d.h. Befähigung und Unterstützung der Nutzer ihre Datenschutzrechte selbst wahrzunehmen und durchzusetzen, soweit möglich,
- Mehrseitige Sicherheit, d.h. es ist kein oder nur minimales Vertrauen in andere Parteien nötig.
- Kontrollmechanismen zur Überwachung der Effizienz der eingesetzten Technologien und Konzepte und der
- „Privacy by Design" (PbD).

Der „Privacy by Design"-Ansatz umfasst Technologien und Konzepte, die nicht reaktiven sondern proaktiven Charakter haben. Sinn und Zweck dieser Ansätze ist es nach Cavoukian (2010), dem Nutzer Möglichkeiten an die Hand zu geben, seine Privatsphäre zu schützen, bevor diese angegriffen wird. Unter anderem soll ein PbD-Konzept dem Nutzer ermöglichen, für seine Daten ein Verfallsdatum, d.h. eine Frist zu definieren, nach der die Daten automatisch gelöscht werden. Daneben soll der Zeitraum für das Speichern unterschiedlicher Informationen differenziert, demzufolge datenbezogen vom Nutzer selbst zu gestalten sein (Mayer-Schönberger 2007; Sterbik-Lamina, Peissl, Čas 2009). Dabei wäre ein proaktives Handeln späterem Nachbessern vorzuziehen.

Vor allem im RFID-Bereich existieren bereits zahlreiche nach diesen Grundsätzen gestaltete Technologien wie z.B. „RFID-Zapper", „Bloggertags", „Tag-Pseudonyms" und sog. „Physically Changing Bits" (Zou 2006; Oertel et al. 2004). Daneben können Technologien auch direkt auf dem PC implementiert werden wie z.B. so genannte Identitätsmanagementsysteme (IMS). Ihre Kernfunktionalität ist die (Un-)Verkettbarkeit von Daten und Teilidentitäten, so dass der Nutzer unbeobachtet von unautorisierten Dritten kommunizieren kann. Der Ansatz der IMS wird schon seit einigen Jahren verfolgt und wurde bereits 2003 in einer von der EU finanzierten und vom Independent Centre für Privacy Protection (ICPP bzw. Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein) durchgeführten Studie untersucht (ICPP 2003). Die Studie setzte sich ausführlich mit technischen, juristischen und soziologischen Problemstellungen auseinander. Bisher konnten sich IMS aber außerhalb der ‚Szene' nicht durchsetzen; Gründe für die fehlende Marktdurchdringung wären u.a. zu untersuchen.

Eine weitere Variante der PET stellen Software-Entwicklungen zum anonymen Surfen, wie beispielsweise Tor[33] oder das sog. JonDonym-System, dar. Das JonDonym-System wurde im Rahmen des von 2000 bis 2006 vom Bundeswirtschaftsministerium geförderten Forschungs- und Entwicklungsprojekts „AN.ON – Starke Anonymität im Internet"[34] entwickelt. Das Programm ermöglicht es, Webdienste über eine IP-Adresse im „JonDonym-System" zu besuchen, und den Datenverkehr so zu verschlüsseln. Hierdurch ist nach Aussagen der Entwickler nicht nachverfolgbar, welche Webseiten aufgerufen werden oder zu welchem Server eine Verbindung aufgebaut wird. Zudem beschäftigen sich seit 2010 Passauer Forscher im Rahmen des vom BMBF geförderten Projektes „inSel" – informationelle Selbstbestimmung in Dienstenet-

[33] http://www.torproject.org
[34] http://anon.inf.tu-dresden.de

zen – damit, „den Datenverarbeiter als unerwünschten Mitwisser auszuschalten“ (Becker 2010). Beim Prototyp des „inSel“-Projektes hinterlegt der Nutzer seine Daten in einem verschlüsselten Datentresor auf den Dritte nur dann Zugriff erhalten, wenn der Nutzer es ausdrücklich gestattet. Der Datenverarbeiter sieht somit nur die verschlüsselten Daten.

Unverzichtbar für den Schutz der Privatsphäre sind darüber hinaus Verschlüsselung mit hinreichend langen Schlüsseln, gute Zufallsgeneratoren und geeignete Algorithmen, sowie Endgeräte, die den Missbrauch privater Informationen, wie Passwörter, verhindern (sichere Endgeräte, Smartcards).

2.2 Folgedimensionen

In den folgenden Kapiteln werden potentielle Folgen dargestellt, wie sie in ITA- und Fachkreisen diskutiert werden, also z.B. von Fachleuten aus Ministerien und Parlamenten, Datenschutzorganisationen, Forschern (bspw. Kryptologen und Betriebswirten), Marktanalysten und Unternehmen. Die breite Erfassung von Meinungen und Forschungen dient dazu, möglichst viel Wissen über potentielle, insbesondere nicht-intendierte Folgen zu sammeln.

2.2.1 Allgemeines

Sowohl Web 2.0 Dienste, Mobile und Ubiquitous Computing als auch Lokalisierungsdienste sind heute, zum einen in einigen Anwendungsbereichen Realität, zum anderen befinden sie sich teilweise noch im Pilotstadium. Sie haben aber bereits u.a. die Gesellschaft beeinflusst und nach Aussagen von Journalisten, aber auch von Forschern zu neuen Wirtschaftszweigen wie z.B. Data Brokern geführt (ZDF 2010; Čas, Peissl 2010). Experten sind aber der Überzeugung, dass sich die heute noch visionären IT-Szenarien in vielen Anwendungsbereichen in den kommenden Jahren zunehmend durchsetzen werden (Friedewald 2009a). Eine der wichtigsten Herausforderungen könnte dabei sein, die sozialen Werte und Grundrechte wie den Schutz der Privatsphäre oder das selbstbestimmte Handeln nicht zu gefährden.[35]

Welche dynamische Entwicklung in kurzer Zeit möglich ist, und welche Auswirkungen dies auf das wirtschaftliche, gesellschaftliche und politische Leben hat, haben beispielweise die Verbreitung und Anwendung des Internets und des Mobilfunks gezeigt. Aufgrund der Heterogenität der Anwendungsfelder und der Technologien ist eine Vielzahl von Zukunftsvisionen möglich, die sowohl positiv als auch negativ interpretiert werden können. So werden schon seit einigen Jahren Szenarien einer schöneren und besseren Welt (Aarts, Marzano 2003) als auch Szenarien einer totalen Überwachungsgesellschaft (Albrecht, McIntyre 2005) diskutiert.

Im Folgenden wird eine kurze Übersicht über die potentiellen positiven und negativen Auswirkungen von Web 2.0 Diensten, Kommunikationstechniken, Lokalisierungsdiensten sowie der Vision einer allgegenwärtigen Datenverarbeitung gegeben.

Aufgrund der thematischen Einschränkung der Kurzstudie auf den Umgang mit sensiblen, personenbezogenen Daten und den Einfluss der behandelten Technologie-Konzepte auf die informationelle Selbstbestimmung wird in der Diskussion der intendierten und nicht-intendierten Nebenfolgen auf eine Vielzahl von Potentialen und auf einige Folgedimensionen der vorgestellten technologischen Konzepte verzichtet. Beispielsweise entfällt eine Betrachtung ökologischer Aspekte. In den folgenden Kapiteln stehen deswegen Fragen zur informationellen Selbstbestimmung, zum Datenschutz und zur Privatsphäre im Mittelpunkt.

[35] Aussage eines Experten im Rahmen des im November 2009 durchgeführten Experten-Workshops.

2.2.2 Gesellschaftliche/ Soziale Dimension

Besonders die Bedeutung von Web-basierten **Sozialen Netzwerken** (SNS) im Internet ist in den letzten Jahren kontinuierlich gestiegen. Die bekanntesten Anbieter Facebook, Xing und MySpace ziehen nach eigenen Angaben weltweit jeden Monat jeweils mehr als 100 Millionen Besucher auf ihren Webseiten an und gehören damit zu den am stärksten wachsenden Diensten im Internet (Heidemann 2009; Weiß 2010a). Dienste wie Twitter ermöglichen einen Austausch von Informationen zu jeder Zeit und an jedem Ort. Auch in Unternehmen dienen SNS inzwischen zum Austausch von Informationen und zur Unterstützung von Zusammenarbeit (Koch, Richter, Schlosser 2007; Cyganski, Hass 2008; Smith et al. 2009).

Richter und Koch (2008) konstatierten bei den Social Networking Diensten große Forschungslücken, da ihrer Ansicht nach zum einen die Form von Social Software relativ jung ist und andererseits die Entwicklungsgeschwindigkeit der Dienste enorm schnell. Seither wurde die Problematik jedoch in einigen Veröffentlichungen und Studien aufgegriffen und in Projekten[36] wie u.a. dem von der EU geförderten Projekt „Primelife“[37] untersucht.

Grundsätzlich weisen Experten darauf hin, dass der Nutzer, dessen persönliche Informationen und die mit seinem hinterlegten Profil verbundenen Daten und Verbindungen zu anderen Personen im Fokus Sozialer Netzwerk Anwendungen stehen (Weiß 2010b).

> *„When people join social networking sites, they begin by creating a profile, then make connections to existing friends as well as those they meet through the site. A profile is a list of identifying information. It can include your real name, or a pseudonym. It also can include photographs, birthday, hometown, religion, ethnicity, and personal interest. Members connect to others by sending a "friend" message, which must be accepted by the other party in order to establish a link. "Friending" another member gives them access to your profile, adds them to your social network, and vice versa"* (Dwyer, Hiltz, Passerini 2007).

Nach der Ansicht von Experten könnte sich positiv gesehen das Internet so neben der Befriedigung der Kommunikations- und Mitteilungsbedürfnisse zu einer Art ‚Gedächtnis der Alltagskultur' entwickeln, da eine Vielzahl an Informationen selbst nach deren Löschen noch jahrzehntelang im Netz abrufbar sind. In der Literatur finden sich aber vielfache Hinweise zu daraus entstehenden Nachteilen, die teilweise auch in der aktuellen politischen und öffentlichen Debatte diskutiert werden (Mayer-Schönberger 2008; ; Sterbik-Lamina, Peissl, Čas 2009): Sind diese Daten erst einmal verfügbar, bleiben sie nahezu unbegrenzt gespeichert und man kann sich (so schnell) nicht mehr von seinen Internet-Identitäten lösen; die Identitäten ‚kleben' an den Nutzern. SNS-Nutzern fehlen aber nach Meinung von Experten die technischen und rechtlichen Grundlagen, um ihre personenbezogenen Daten effektiv zu schützen, d.h. sie auf Wunsch z.B. zu korrigieren oder auch dauerhaft zu löschen. Zudem werden nach Überzeugung vieler Datenschützer und Forscher die Gefahren von der Veröffentlichung der eigenen Person oft noch unterschätzt. Schon seit einigen Jahren wird in diesem Kontext diskutiert, dass es eine Diskrepanz zwischen dem Wunsch nach Privatsphäre und dem ‚öffentlichen' Verhalten in SNS zu geben scheint (Acquisti 2006; Ismail 2010; Buhl, Müller 2010; Mainusch, Burtchen 2010). S. B. Barnes (2007) nannte dieses Phänomen, das ‚Privacy Paradoxon'. Auch die Studien „Web 2.0 als Rahmen für Selbstdarstellung und Vernetzung Jugendlicher" (Sain 2009) und „Chancen und Gefahren von Online Communities" (Sain 2010) indizieren, dass Jugendliche eher einen ‚pragmatischen' Umgang mit dem Faktor Privatsphäre zu haben scheinen. Diese Form des Umgangs mit Daten birgt nach Aussagen von Experten in sich bereits Gefahren für den Schutz der persönli-

[36] Beispielsweise startete am 1. September 2010 das Projekt des Center for Advanced Studies and Research in Information and Communication Technologies & Society der Universität Salzburg zu „Social Networking Seiten in der Überwachungsgesellschaft".

[37] http://www.primelife.eu

chen Daten (Rannenberg, Kahl, Böttcher 2010; Weiß 2010b)[38]. Hierdurch werden Datenschützer nach Holtz (2010) und Bizer (2007) vor ein grundsätzliches Problem gestellt: Die Dichotomie der SNS, ‚Öffentlichkeit' einerseits und ‚Privatheit' andererseits, stellt zwar keinen unmittelbaren Widerspruch zu den Grundprinzipien des Datenschutzes dar, sie macht es aber schwieriger, ein datenschutzkonformes Social Networking zu ermöglichen. Daneben weisen einige Sicherheitsforscher auf Sicherheitsmängel und Schwachstellen, der in SNS implementierten Softwareprogramme hin (Fraunhofer 2008; Weiß 2010b). 2010 veröffentlichte die Europäische Kommission in diesem Zusammenhang die Ergebnisse eines unabhängigen Gutachtens zur Implementierung der „Safer Social Networking Principles for the EU" (Euro 2010). Im Rahmen des Gutachtens wurde die Umsetzung der Grundsätze für eine sichere Nutzung sozialer Netzwerke durch 20 der größten in Europa operierenden Anbieter überprüft. Ergebnis war, dass lediglich zwei der 20 getesteten Anbieter alle Grundsätze erfüllen. Zudem sind nach einer Studie des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) gesamtheitliche, konsistente und klare Konzepte zum Privatsphärenschutz bei SNS nur begrenzt auszumachen (Fraunhofer 2008). Projekte wie „Privacy and Identity Management for Community Services (PICOS)[39] forschen aber derzeit daran, wie Datenschutz und Privatsphäre in SNS verbessert werden und der Umgang mit sensiblen/ personenbezogenen Daten gesellschaftlich konsensuell erfolgen könnte.

Doch nicht nur der Nutzer selbst schafft sich nach Aussagen der Experten seine digitale Identität. Durch die teilweise unwissentliche Verlinkung von Bildern und die Veröffentlichung von Artikeln, Zitaten oder auch Gerüchten, welche durch Suchmaschinen auffindbar sind, gibt der Nutzer seine Identität ein Stück weit in die Hände anderer. Das heißt, er schafft sein digitales Profil nicht selbst, es wird (stärker als in der realen Welt) von anderen Nutzern mitgeschaffen.

Nach Auffassung von Karla (2010) wird durch diese Nutzung der Daten in anderen als für die Entstehung implizierten Zusammenhängen, der Möglichkeit der Fehlinterpretation und des Missbrauchs das Problem der informationellen Selbstbestimmung und des Datenschutzes noch verschärft.

Daneben weisen einige Experten darauf hin, dass neben den bei den SNS von den jeweiligen Nutzern freiwillig zugänglich gemachten und gespeicherten personenbezogenen Daten, im Netz auch Daten von Nutzern gespeichert werden, die dieser nicht wissentlich ins Netz gestellt hat. So werden beispielsweise nach Stern, Böhm und Buchmann (2010) durch die Betreiber von **kollaborativen Suchmaschinen** Recherchegewohnheiten der Nutzer aufgezeichnet, aus denen u.a. Informationen für soziale Profile gewonnen werden können (‚Social Profiling'). Dabei wird nicht nur die Suche nach einem Online-Lieferservice, dem Kinoprogramm o.ä. archiviert, sondern auch die Suche nach einem Kreditinstitut, einer Samenbank oder zu konkreten Krankheitsbildern[40]. Dies gilt aber nicht nur für Einzelpersonen, sondern ebenso für Unternehmen, deren Mitarbeiter möglicherweise unbeabsichtigt wichtige Geschäftsgeheimnisse durch die Eingabe artverwandter Begriffe preisgeben. Alle diese Daten können gesammelt, mit Zusatzdiensten verkettet[41], ausgewertet und zum Teil verkauft werden. Hierfür stellen IP-Adressen, Session-IDs und Cookies wesentliche Grundlagen dar.

---

[38] In einer der ersten wissenschaftlichen Studien zu SNS und Privatsphäre wurden im Jahr 2005 4.000 Facebook-Profile analysiert und dabei die potentiellen Bedrohungen der Privatsphäre durch eine Rekonstruktion der Sozialversicherungsnummer alleine mithilfe der bei Facebook angegebenen personenbezogenen Daten unterstrichen.

[39] Das Projekt PICOS wird seit 2008 für 36 Monate von der Europäischen Union gefördert. Nähere Informationen unter http://www.picos-project.eu

[40] Nach Hilty et al. (2003) informieren sich immer mehr Patienten über Krankheiten mit Hilfe des Internets (Suchmaschinen).

[41] Die Verkettung digitaler Identitäten wurde im Zeitraum 11/2006 bis 07/2007 durch das Projekt „Verkettung digitaler Identitäten", das vom Bundesministerium für Bildung und Forschung im Rahmen der Innovations- und Technikanalyse (ITA) gefördert wurde, untersucht.

Experten gehen davon aus, dass es Nutzern meistens nicht bewusst ist, dass alle diese personenbezogenen Daten zur Erstellung von umfassenden Persönlichkeitsprofilen (Dritsas, Tsaparas, Gritzalis 2006) verwendet werden (Boyd, Ellison 2007; Buhl, Müller 2010; ENIS 2010a), die nach Čas (2010) inzwischen zu einem Wirtschaftsgut geworden sind und zur Geburt von neuen Werbeformen (personalisierte Werbung mit dynamischer Preisfindung) und zu neuen Wirtschaftszweigen wie Data Brokern oder Reputation Management-Unternehmen. Ein Bericht des Auslandjournals (ZDF 2010) aus dem Jahr 2010 zeigt daneben, dass der freie Umgang mit Daten auch zu sozialen Effekten wie „Mobbing im Internet" und neuen Formen von Kriminalität[42] geführt haben.

Deswegen fordern Studien und Positionspapiere der Europäischen Agentur für Netzwerksicherheit (ENISA, ENISA 2010a; ENISA 2010b; ENISA 2010c) und öffentliche Stellungnahmen der Internationalen Konferenz der Datenschutzbeauftragten[43] neben Programmen zur Erhöhung des Bewusstseins im sensiblen Umgang mit persönlichen Daten, technische Lösungen bezüglich des Datenschutzes von SNS. Die öffentlichen Positionen sind dabei aber meist auf allgemeine Vorschläge und Gedanken zum Verbraucherschutz und des Schutzes Minderjähriger und Jugendlicher beschränkt. Risiken für die Privatsphäre aller Altersgruppen und technische Lösungsvorschläge werden nicht benannt.

Betrachtet man neben den, in Abschnitt 2.1 sehr knapp und beispielhaft beschriebenen, Anwendungsmöglichkeiten, die Vorteile der oben beschriebenen technologischen Konzepte, so ist ihnen allen gemein, dass sie Vorgänge vereinfachen und den Menschen in vielen Bereichen (Wohnen, Arbeit und Wirtschaft, Freizeit, Einkauf, Reisen und Verkehr sowie dem Gesundheitswesen) unterstützen könnten. Außerdem könnten sie die Initialisierung und Vereinfachung automatisierter Abläufe, die Erleichterung von Arbeitsgängen sowie u.a. ein selbstbestimmtes Leben (vgl. dazu Ambient Assisted Living, AAL)[27] ermöglichen.

Bei dem Einsatz von **RFID-Technologien** sollte in vielen Anwendungsbereichen unterschieden werden, ob diese nur für den intendierten Zweck, z.B. im Fall des ePasses zur Identifikation einer Person, verwendet oder auch in nicht-intendierter Weise durch die Verknüpfung mit anderen persönlichen Daten des Kunden z.B. mit Hilfe von Kunden- oder Kreditkarten genutzt werden. Durch derartige Zweckentfremdung ist nach Roßnagel und Müller (2004) eine Erstellung von umfassenden und detaillierten Persönlichkeitsprofilen möglich, die u.a. eine Beurteilung der Persönlichkeit erlauben und damit eine Gefahr für die informationelle Selbstbestimmung darstellen. Ebenso wie bei den oben bereits genannten SNS und Suchmaschinen sowie bei Mobiltelefonen oder anderen Endgeräten, halten es Ray (2008) und Bizer et al. (2006) für bedenkenswert, dass Bürger in der Regel keine Kenntnis von und keine Einflussmöglichkeit auf die im Hintergrund ablaufenden Analysen und Verkettungsprozesse haben.

Beim **Ubiquitous Computing** werden durch die Ausstattung von Produkten, Tieren, Personen und der gesamten Umgebung mit RFID-Chips und/ oder Sensoren Daten erhoben, verarbeitet und genutzt. Dabei führt nach einer Studie im Rahmen des EU-Projektes „Safeguards in a World of Ambient Intelligence (SWAMI)" die Allgegenwärtigkeit und die ‚vermeintliche' Unsichtbarkeit der Technik wie z.B. Auto-Identifikationsnummer, auf Distanz arbeitende Sensoren oder Videokameras zu einer Vervielfachung der erhobenen (digitalen) Daten (Punie et al. 2006) und zu einer vollkommen neuen Qualität des Datenpools. Dadurch, dass immer mehr Prozesse autonom ablaufen, könnte es im Einzelfall jedoch zu Kontrollverlusten kommen und selbstbestimmtes Handeln u.a. erschwert werden. Alltagsgegenstände bekommen quasi einen eigenen Willen und die daraus resultierenden Vorgänge sind für den Nutzer oft intransparent und nicht nachvollziehbar. Diese Tatsache könnte durch die unkontrollierte, unbegrenzte, vom Einzelnen nicht gewollte Erhebung, Speicherung, Übermittlung und Nutzung seiner personenbezogenen Daten im worst-

[42] In England wurde eine 17-Jährige ermordet, nachdem sie sich mit einer vermeintlich 16-Jährigen Facebook-Bekanntschaft getroffen hatte. Hinter dem Profil des 16-Jährigen versteckte sich in Wirklichkeit ein 32-Jähriger Sexualtäter (ZDF 2010).

[43] vgl. dazu Pressemitteilungen unter http://www.datenschutz-berlin.de/content/nachrichten/pressemitteilungen

case-Szenario zu einer ‚Potenzierung' der eben dargestellten Nebenfolgen und wiederum zu einer Beschädigung des Rechts auf informationelle Selbstbestimmung führen. Eine neue Dimension für den Datenschutz ergibt sich nach Ansicht von Experten durch die Erstellung individueller Personenprofile, die automatisierte Rückschlüsse durch Verkettung von Sensordaten und nicht personenbezogenen und öffentlich zugänglichen, statistischen Daten, zulassen. Ein Beispiel dafür stellen Datamining-Systeme dar, mithilfe derer komplexe Profile erstellbar sind (Bizer et al. 2006; Friedewald, Lindner 2008; Hildebrandt, Gutwirth 2008; Friedewald et al. 2009b).

In diesem Zusammenhang ist eine gesellschaftliche Diskussion über die Herausforderungen und Anforderungen aller hier angeführten technologischen Konzepte bezüglich des Datenschutzes zu erwarten, die wissenschaftlich begleitet und gefördert werden könnte. Darüber hinaus sollte nach Meinung der European Network and Information Security Agency (ENISA) untersucht werden, ob Menschen jeden Alters ein zweckmäßigeres Datenschutzbewusstsein[44] vermittelt werden müsste und ihnen Technologien zum Schutz der Privatsphäre (Privacy Enhancing Technologies) an die Hand gegeben werden sollten, um ihnen damit die Kontrolle und die Verfügungsmacht über die eigenen Daten zurückzugeben. Ein schnelles Handeln aller Akteure, vor allem aber des Staates könnte nach Angaben von Experten angeraten sein, bevor die Auswirkungen auf das Grundrecht zur Wahrung der Privatsphäre nicht mehr reversibel sind[45].

2.2.3 Folgen von Lokalisierungsdiensten

Mobile Web 2.0-Angebote und (standortbasierte) Lokalisierungsdienste (**Location Based Services**), die mithilfe positionsabhängiger Daten die reale und virtuelle Welt verbinden, ermöglichen neben den in Abschnitt 2.1.4 beschriebenen standortbasierten Dienstleistungen auch die Lokalisierung von Freunden, von Unfallopfern oder Arbeitnehmern durch Ortung des Mobiltelefons oder eines RFID-Chips in der Kleidung. In einer Studie der TA-SWISS wird daneben auch noch der Aspekt der Verbrechensbekämpfung angesprochen (Hilty et al. 2003), so könnten z.B. ‚entführbare' Personen oder auf Bewährung freigelassene Sträflinge geortet werden (COMM 2009; Hickman et al. 2010). Zwar sind LBS, die beispielsweise auf dem GPS-System beruhen, für viele Anwendungen noch zu groß, zu teuer, zu ungenau und nicht energieeffizient, dennoch erzielt man bei allen vier Parametern kontinuierliche Fortschritte. So steigt der Anteil der verkauften GPS-fähigen Mobiltelefone rapide an[46] und ermöglicht eine immer größere Reichweite der LBS. Je genauer und einfacher der Ort eines kleinen, preiswerten Gerätes ermittelt werden kann, umso zahlreicher und vielfältiger können die denkbaren Anwendungen sein. Dadurch könnten nach Aussagen von Mattern (2005) jedoch auch die Missbrauchsgefahren und die potentiellen Eingriffsmöglichkeiten in die lokale Privatsphäre (‚location privacy') wachsen.

Neben der besseren Verfügbarkeit und den von Nutzern positiv wahrgenommenen neuen Anwendungsmöglichkeiten der LBS sollten nach Ansicht von Datenschützern aber die Möglichkeiten, immer zu wissen, an welchem Ort sich Bekannte, Freunde und Mitarbeiter aufhalten, mit großer Skepsis betrachtet werden. Beispiele dafür wären die Überwachung von Kindern oder Ehepartnern, die schnell in eine Kontrolle von Menschen umschlagen könnte (Stichworte: Human- und Handy-Tracking). In diesem Kontext wären diese nicht-intendierten Auswirkungen zu untersuchen und ein sinnvoller Umgang mit „Tracking- und Tracing"-Anwendungen zu erarbeiten. Neben der Ortung von Personen können Lokalisierungsdienste auch für orts- und personenbezogene Werbemaßnahmen und Dienstleistungen (vgl. Kapitel 2.1.4,) verwendet werden. Die Artikel-29-Datenschutzgruppe veröffentlichte diesbezüglich im Juni 2010 eine „Opinion" zum Thema

[44] Oft auch unter dem Begriff „internet literacy" zu finden.

[45] Aussagen im Rahmen des im November 2009 durchgeführten Experten-Workshops.

[46] Schon heute haben über 50% der neu ausgelieferten Handys einen GPS-Sender integriert, dieser Anteil soll bis Ende 2011 auf ca. 80% ansteigen. Näheres unter http://www.isuppli.com/Mobile-and-Wireless-Communications/News/Pages/Four-out-of-Five-Cell-Phones-to-Integrate-GPS-by-End-of-2011.aspx

„online behavioural advertising“ (Art 2010). Diese Dienste werden zusätzlich noch durch mobile Applikationen (Apps) unterstützt, die Unternehmen erlauben, Verbraucher zu Filialen in der Nähe zu lenken, und diese gleichzeitig über ihr Produktangebot zu informieren.

In Kombination könnten die im Abschnitt 2.1 genannten Technologien und Konzepte die Möglichkeit bieten neben dem Verbrauchs- und Interessenprofil noch zusätzlich ein Bewegungsprofil d.h. ein komplettes Persönlichkeits- oder Lebensprofil einzelner Personen zu erstellen. Im Zusammenhang mit den Datensammlungen wird deswegen von Dobson und Fisher (2003) sogar angemahnt, dass diese zu einer Machtkonzentration und neuen Formen von Sklaverei („Geoslavery“) führen könnten. Hennig, Ladkin und Sieker (2004) und Sieker und Ladkin (2005) formulieren es so: „Denn wer auch immer Zugang zu deren Daten hat, hat Macht über die Bürger“. Daneben sehen Experten in den zunehmenden Überwachungsmöglichkeiten auch die Gefahr eines wachsenden Misstrauens zwischen Menschen, wobei es nach ihrer Auffassung von spezieller Bedeutung ist, ob z.B. ein RFID-Implantat freiwillig getragen wird oder unter Zwang eingesetzt wurde (Anderson, Labay 2006; Lieshout, Kool 2008). Befürworter gehen dagegen davon aus, dass datenschutzrechtliche Bedenken für Verbraucher dann in den Hintergrund treten, wenn sie einen Nutzen z.B. von den LBS erhalten („Nutzen-Kosten-Kalkül „) (Kölmel, Hubschneider 2003)[47].

Datenschutzorientierte Experten sind der Überzeugung, dass die Möglichkeiten, die sich durch die allgegenwärtige und oft (nahezu) unsichtbare Überwachung und Lokalisierung ergeben, gravierend in das komplexe Gleichgewicht von Freiheit und Schutz einerseits, Überwachung und Privatsphäre andererseits eingreifen. Laut Mattern (2005) kommt gerade der „location privacy“ bezüglich des Schutzes der Privatsphäre eine besondere Bedeutung zu. Die European Network and Information Security Agency (ENISA) vertritt dabei den Standpunkt, dass, wenn persönliche Dinge ‚wissen', wo sie sind, oder gespeichert haben, wo sie waren, es ein Leichtes ist, auf den Aufenthaltsort und die Wege einer Person, Rückschlüsse zu ziehen und diese zu überwachen (ENISA 2010b)[48].

Die Rolle des ‚großen Bruders'[49] können dabei sowohl in- und ausländische Regierungen und Geheimdienste spielen, wie auch große Unternehmen. Dabei wäre z.B. an einen möglichen Zugriff auf Server US-amerikanischer Cloud-Computing-Provider zu denken. Durch das Verketten und Verlinken der einzelnen, von den verschiedensten Technologien ermittelten, gesammelten, aufgezeichneten oder gespeicherten Informationen, lassen sich Bewegungs-, Verbrauchs- und damit auch Interessenprofile ableiten, die z.B. als Grundlage für eine gezielte, d.h. auf den Einzelnen zugeschnittene Werbung (personalisierte Werbung), fungieren. Kuhlen (2004) u.A. haben im Zusammenhang mit personalisierter Werbung, personalisierten Dienstleistungen und E-Commerce einen Trend festgestellt, der die Privatsphäre nicht mehr als absolute Voraussetzung für ein selbstbestimmtes Leben betrachtet. Vielmehr scheint sie nach Meinung von Klüver et al. (2006) zu einem Verhandlungsgegenstand und einem in Teilen aufgebbaren Gut zu werden, wenn daraus genügend materielle Anreize oder mehr Komfort resultieren.

---

47 Im Rahmen des von der Europäischen Kommission geförderten Forschungsprojektes ELBA (European Location Based Advertising) wurden die Erwartungen, Anforderungen, Hemmschwellen und Barrieren potentieller Nutzer von LBS identifiziert. Für weitere Informationen siehe www.e-lba.com

48 In diesem Kontext wurde vor kurzem sehr kontrovers der Patentantrag zu „Systeme und Verfahren zum Identifizieren nicht-autorisierter Nutzer eines elektronisches Geräts“ (www.pat2pdf.org/patents/pat20100207721.pdf) von Apple diskutiert. In der Presse als „Spy-Phone“ bezeichnet, soll zukünftig eine Software, z.B. anhand von Mitschnitten der Stimme, einer Protokollierung des Herzschlages und der Aufnahme eines Fotos, feststellen, ob das Gerät noch von seinem Eigentümer oder evtl. von einem Dieb benutzt wird.

49 Bezieht sich auf den großen Bruder („Big Brother“) aus dem Roman „1984“ von George Orwell, den vermeintlichen Diktator des fiktiven, totalitären Staates „Ozeanien“, der seine Bürger überwacht und bei Fehlverhalten unterdrückt und foltert bzw. sogar tötet.

2.2.4 Umgang mit personenbezogenen Daten im Gesundheitswesen

Digitale Patientendaten, wie sie z.B. in digitalen Patientenakten oder auf der elektronische Gesundheitskarte (eGK) gespeichert sind, stellen aus der Sicht von einigen Experten bei nicht-intendierter Nutzung eine Gefahr für die informationelle Selbstbestimmung der Betroffenen dar (Borchers 2008; Čas 2008; Dix 2009). Derart erfasste Daten in Kombination mit als riskant oder ungesund identifizierten Lebensgewohnheiten sind u.a. für die Erstellung von Risikoprofilen durch Versicherungsgesellschaften von größtem Interesse. Bei einem Lebensstil, der von der Versicherung als riskant klassifiziert wird, würde dann beispielsweise ein höherer Versicherungsbeitrag fällig. Des Weiteren ist nach Beckwith (2003) und Bick, Kummer und Rössig (2008) zu bedenken, dass sich viele der erhobenen Daten auch für Sekundärzwecke nutzen lassen; dies schließt natürlich auch sinnvolle Nutzungen, wie die Nutzung für Forschungszwecke, ein.

Grundsätzlich muss nach Expertenaussagen berücksichtigt werden, dass sensible, personenbezogene Patientendaten dezentral auf Servern, medizinischen Geräten oder auf persönlichen Endgeräten gespeichert werden. Da teilweise ein Austausch der Daten erforderlich ist, müssen die Speicherorte sowie die (drahtlosen) Übertragungswege gegen unbefugten Zugriff oder unbeabsichtigte Weitergabe an z.B. Besucher oder Mitpatienten, abgesichert sein. Unverschlüsselter Transport führte bereits zu Datendiebstahl wie in Großbritannien (Friedewald et al. 2009b, S. 95).

In diesem Bereich sollte analog zur eGK ein effektiver und autorisierter Zugriff auf die Patientendaten sichergestellt werden. Dies könnte z.B. über eine doppelte Autorisierung durch den Versicherten und den Zugriffsberechtigten erfolgen. Neben den grundsätzlichen datenschutzrechtlichen Bedenken bezüglich der Speicherung und Übermittlung von Patientendaten, sprechen sich manche Datenschützer dennoch für eine Einführung der elektronischen Gesundheitskarte aus. Nach Ansicht des Datenschutzbeauftragten des Landes Schleswig-Holstein Thilo Weichert (2009) könnte somit evtl. auch dem aktuellen laxen Umgang mit Patientendaten beizukommen sein. Daneben sehen manche Experten die eGK geradezu als „Modellvorhaben“, das die „Anforderungen des informationellen Selbstbestimmungsrechts vorbildlich umsetze“ (Gundermann 2008). Inwiefern diese Aussage stimmt oder ob die datenschutzrechtlichen Bedenken angebracht sind, wäre zu überprüfen. J. Čas (2008) empfiehlt deshalb beispielsweise, stets streng zu evaluieren, ob das „doppelte Heilsversprechen“, der besseren medizinischen Versorgung bei gleichzeitig geringeren Kosten tatsächlich erfüllt wird, und damit etwaige Einschränkungen des Datenschutzes überhaupt zu rechtfertigen wären.

2.2.5 Technische Dimension

Um potentiellen Gefahren für die informationelle Selbstbestimmung genauso entgegenwirken zu können wie der potentiell allgegenwärtigen Überwachung, sollten nach Auffassung von Sicherheitsforschern und Datenschützern einige technisch-konzeptionelle Maßnahmen entwickelt werden, die durch rechtliche Rahmenbedingungen durchgesetzt werden könnten.

Das würde grundsätzlich die Schaffung von Wahlmöglichkeiten und Technologien, die z.B. eine Pseudo- oder Anonymisierung, Unverkettbarkeit und eine Verschlüsselung der Daten sicherstellen, umfassen. Daneben müsste nach Meinung von einigen Experten die Verwendung von Daten transparent gestaltet werden (Bizer et al. 2006; ETAG 2007; Weiß 2008) und ein vom Bürger einfach zu bedienender und kontrollierbarer, sicherer Schutz der Privatsphäre realisiert werden (u.a. PET, PIA, PPSSI, Nutzergesteuertes Identitätsmanagementsystem (ENIS 2010b) und Qualitätssicherung). Bedingung hierfür könnte das Kennzeichnen von Geräten und Systemen sein, die potentiell zur Überwachung eingesetzt werden können und mit denen der Nutzer in Berührung kommt. 2007 hat die Europäische Kommission dies bereits für RFID-Transponder empfohlen (Euro 2007). Daneben werden schon seit längerem eine Reihe von Lösungsansätzen wie die Zerstörung oder die zeitweise Deaktivierung von RFID-Transpondern (‚Schlafmodus’) diskutiert (Henning,

Ladkin, Sieker 2004; Sieker, Ladkin, Henning 2005). Zudem wird über eine standardmäßige Off-Funktion nachgedacht, die für die gewünschte Benutzung einer expliziten Bestätigung bedarf (Klüver et al. 2006).

In der aktuellen Debatte wird neben vielen anderen Konzepten diskutiert, dass es dem Nutzer ermöglicht werden sollte, für seine Daten ein Verfallsdatum, d.h. eine Frist zu definieren, nach der die Daten automatisch gelöscht werden bzw. dem Nutzer ein Recht einzuräumen, jederzeit auf seine Daten zugreifen und sie auch löschen zu können (Redi 2010). Daneben müsste der Zeitraum für das Speichern unterschiedlicher Informationen differenziert werden, demzufolge, datenbezogen vom Nutzer selbst zu gestalten sein (Mayer-Schönberger 2007; Sterbik-Lamina, Peissl, Čas 2009; de Maizière 2010).

Darüber hinaus wurden im Rahmen des Projekts „PRISE" Kriterien für die Entwicklung, Implementierung und Nutzung von Privacy Enhancing Technologies erarbeitet (Raguse et al. 2008). Seit 2009 analysiert außerdem das Projekt „Privacy reloaded" des österreichischen Instituts für Technikfolgen-Abschätzung (ITA) sowohl moderne Konzepte des technischen Datenschutzes unter dem Stichwort „Privacy by Design" als auch neuere Ansätze von (Selbst)-Regulierungsmechanismen und beobachtet ihre Einführung.[50]

2.2.6 Ökonomische Dimension

Informationen gelten als wichtige Ressource unserer Zeit und sind inzwischen zu einem Wirtschaftsgut geworden. Kundendaten einen konkreten Wert zuzuschreiben, ist jedoch sehr schwierig, da man zumeist auf Schätzungen angewiesen ist (Čas 2010).

Was Daten heutzutage für einen Wert besitzen können, sieht man auch an der Firma „DoubleClick", einen der größten Anbieter für Online-Marketing-Lösungen, der 2007 für 3,1 Milliarden USD von Google übernommen wurde. DoubleClick hat seit Firmengründung rund 120 Millionen Profile erstellt. Durch den Kauf einer amerikanischen Direktmarketing Agentur von Google konnten innerhalb kürzester Zeit einige hunderttausend bis dahin anonyme Internetnutzer identifiziert werden (Čas 2010).

Daneben wird von Marktanalysten auch SNS ein großes Marktpotential zugeschrieben: „Social network advertising is getting renewed attention in 2010" (Williamson 2010). Die Marktforscher von eMarketer prognostizieren für 2011 weltweite Ausgaben für Werbung in sozialen Netzwerken von 4,3 Milliarden USD (Prognose 2010: 3,3 Milliarden USD). Im Jahr 2010 erhält nach Aussagen von eMarketer Facebook alleine 1,3 Milliarden USD von Werbeunternehmen. Dies entspricht der Hälfte aller Erlöse aus Werbeeinnahmen in den USA und 39 % der weltweiten Werbegelder für soziale Netze. Dagegen verliert nach Prognosen von eMarketer MySpace an Wichtigkeit: 297 Millionen USD in 2010; 2009 waren es noch 347 Millionen USD. Twitter steigt erst 2010 ins Werbegeschäft ein, wobei rd. 50 Millionen USD Werbeeinnahmen prognostiziert werden, allerdings mit großem Potential für die nächsten Jahre (Williamson 2010).

Auch bestimmte RFID-Anwendungsbereiche wie z.B. Ticketing und ÖPNV verzeichnen heute bereits sehr gut Zuwächse. Die vom Bundesministerium für Wirtschaft und Technologie in Auftrag gegebene Studie „RFID: Potentiale für Deutschland" betont, dass RFID kurzfristig zwar eine Rationalisierungstechnologie darstellt, mittel- und langfristig den Anwendern jedoch das Angebot neuer Produkte und Dienstleistungen erlaube (VDI 2007). Damit trage sie „nachhaltig zur Stärkung der Innovationskraft deutscher Unternehmen bei". Nach Ansicht von Fransen (2010) hingegen kann flächendeckend für Deutschland nicht von immensen Steigerungsraten gesprochen werden. Der Marktanalyst IDTechEx prognostiziert dem ungeachtet, dass sich bis 2019 der RFID-Markt von geschätzten 5,56 Milliarden USD in 2010 auf 27,59 Milliarden USD nahezu verfünffachen wird. Laut Aussagen der Marktanalysten werden in immer mehr Unternehmen und öffentlichen Verwaltungen funkgesteuerte Etiketten für das Identifizieren oder Lokalisieren von Gegen-

[50] Für weitere Informationen, http://www.oeaw.ac.at/ita/ und aktuelle Projekte.

ständen eingesetzt, so z.B. in 2010 rund 800 Millionen RFID-Label allein im Bekleidungssektor (Williamson 2010).

> *„However, the biggest spenders are still governments, who are able to implement large RFID schemes such as animal tagging, transit ticketing, people identification etc."* (Das, Harrop 2010).

Dies lässt darauf schließen, dass diverse Techniken des Ubiquitous Computing mittel- und langfristig von großer wirtschaftlicher Bedeutung sein könnten und zu grundlegenden Veränderungen in Geschäftsprozessen führen könnten, da zusätzliche Services und neue Geschäftsmodelle möglich würden. Beispielsweise könnten durch das Ermitteln der tatsächlichen Nutzung von Gegenständen und Weitermeldung an Unternehmen neue Abrechnungs- und Leasingmodelle geschaffen werden (Fleisch, Christ, Dierkes 2005). Marktanalysten von Juniper Research prognostizieren in einem aktuellen Report:

> *„[…] revenues from mobile location-based services are expected to reach more than $12.7 billion by 2014"* (Juniper 2010).

Sogar 21,14 Milliarden USD in 2015 erwarten dagegen die Analysten von Global Industry Analysts Inc. für die LBS-Branche (Glob 2010). Während der LBS-Markt bisher keine spektakulären Zuwächse verzeichnen konnte[51], gehen die Analysten davon aus, dass

> *„the increasing availability of GPS handsets and applications (particularly Android and iPhone applications) will help accelerate adoption for LBS across the world. We are forecasting a total addressable global market for GPS navigation and location based mobile services to rise by a CAGR of 51.3 % to $13.4 billion in 2014, from $1.6 billion in 2009. [...] Location Enabled Search and Advertising will see the biggest growth, growing at a CAGR of 131% over the next five years Location Enabled Search and Advertising will replace Voice-guided In-Car Navigation as the main use for GPS-LBS applications in the next several years."* (IEMR 2010).

Die verstärkte Nutzung von Apps wird diesen Trend antreiben. Laut einer Studie von Gartner Inc., wird die Zahl der Apps von 4,5 Milliarden in 2010 auf 21,6 Milliarden Downloads in 2012 mit einem Umsatz von 29,5 Milliarden USD weltweit, ansteigen (Baghdassarian, Milanesi 2009). Dabei sind dann den Erwartungen zufolge 87 % aller Apps kostenlos, da sich der Großteil der Applikation durch innerhalb der Apps geschaltete Werbung für die Unternehmen rechnen wird.

Im Bereich der Wearables hat sich nach Aussagen von Linz vom Fraunhofer Institut für Zuverlässigkeit und Mikrointegration (IZM) „Deutschland längst an die Spitze gesetzt". Hierbei handle es sich nach einem Artikel des Handelsblatts vom Februar 2008 um einen stark wachsenden Markt (Toprak, Kutter 2008).

2.2.7 Politische Dimension

Auch wenn bereits einige rechtliche Rahmenbedingungen wie z.B. das Bundesdatenschutzgesetz (BDSG), die Datenschutzgesetze der Länder, die Datenschutzdirektive 95/46/EG, Art. 29 und 30 §1a, 3, die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG, Art. 15 §3, Artikel 255 EC Treaty, die Verordnungen 45/2001/EG und 1049/2001/EG, der Beschluss Nr. 1247/2002/EG des Europäischen Parlaments sowie die Regulation (EC) No 1049/2001 u.a. existieren, die im Zusammenhang mit informationeller Selbstbestimmung, Datenschutz und Privatsphäre anwendbar sind, sind dennoch nach Aussage von manchen Experten bei der Anwendung aller in der vorliegenden Kurzstudie behandelten technischen Konzepte

[51] Japan ist hier eine Ausnahme, da LBS-Systeme in einem Land ohne Straßennamen sehr nützlich sind, vgl. http://www.navitime.co.jp/en/.

weitere klar definierte rechtliche Regelungen[52] in einem vorausschauenden Rechtssystem notwendig (Stolfo, Tsudik 2010):

> *„What is also needed is a clearly defined policy that governs how entities use, store, and transmit personal data, as well as who is permitted to access it."*

Zukünftig wäre demnach zu untersuchen, welche „weiteren klar definierten Regelungen" erforderlich sind und ob eine Reform des Datenschutzrechts auf europäischer Ebene in Richtung eines ‚codex digitalis" anzustreben ist. In der Studie „Policy options for Radio Frequency Identification (RFID) application in healthcare; a prospective view" finden sich bereits einige Vorschläge für rechtliche Rahmenbedingungen beispielsweise im Gesundheitsbereich (van Oranje-Nassau, Schindler, Botterman 2009). Darüber hinaus votiert der EU-Datenschutzbeauftragte Hustinx dafür, neue Rechtsinstrumente zu erlassen (Heise 2010)[53]. Aber auch internationale Regelungen könnten im Rahmen der Globalisierung und der unterschiedlichen landesspezifischen Datenschutzgesetze anzustreben sein, da es teilweise zur Zeit nicht möglich ist, rechtlich gegen Anbieter von Web 2.0-Diensten vorzugehen[54], da diese im Ausland sitzen. Diese Globalisierung durch das zunehmende Outsourcen von Datentransfer-Prozessen meist außerhalb der EU und eine notwendige Verbesserung des internationalen Datentransfers wird bereits u.a. in der geplanten Novellierung der Datenschutzdirektive 95/46/EG adressiert (Euro 2010). Die Notwendigkeit einer internationalen Vereinbarung von Normen wird auch in einer Studie des TAB erwähnt (Friedewald et al. 2009a). Darüber hinaus wären auch die „National Strategy for Trusted Identities in Cyberspace" (DHS 2010) sowie die Aktivitäten von Microsoft, die nach den „Laws of Identity" eine Verwendung von Pseudonymen und „minimal disclosure" vorsehen (Cameron 2009), zu berücksichtigen.

Einen bereits konkreten Fortschritt im Bereich der Privacy by Design stellt das im April 2011 von der EU-Kommission und Vertretern von Wirtschaft und Verwaltung gemeinsam verabschiedete „Privacy and Data Protection Impact Assessment Framework for RFID Applications" dar (Frame 2011). Die zur Datenschutzfolgeabschätzung (Privacy Impact Assessment, PIA) im Vorfeld der Markteinführung sich selbst verpflichtenden Betreiber von RFID-Anwendungen finden darin konkrete Richtlinien, wie der Prozess einer Datenschutzfolgeabschätzung verlaufen muss, welche Risiken überprüft und welche möglichen Gegenmaßnahmen ergriffen werden müssen. Die Ergebnisse der Datenschutzfolgeabschätzung werden in einem standardisierten PIA-Report festgehalten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit den „Technischen Richtlinien für die Radio-Frequency-Identification-Technologie" (BSI TR-03126, „Sicherer RFID-Einsatz") anwendungsspezifische Erweiterungen (templates) des PIA-frameworks erstellt.[55] Templates sind als zusätzliche Instrumente im PIA-framework ausdrücklich vorgesehen und betreffen spezifizierte Richtlinien für verschiedene Einsatzgebiete von RFID-Anwendungen wie z.B. eTicketing im öffentlichen Personenverkehr, Handelslogistik oder den elektronischen Mitarbeiterausweis. Mithilfe von Datenschutzfolgeabschätzungen dieser Art verpflichten sich Betreiber von RFID-Anwendungen zu einer Analyse ihres Produktes und der Suche nach Verbesserungen des Datenschutzes im Vorfeld der Markteinführung. Durch einen Gewinn an Transparenz in diesem Bereich könnte die Akzeptanz der RFID-Technologie gesteigert werden.

Eine andere Art von Maßnahmen bestehen aus Awareness- und Bildungsaktivitäten, wie z.B. schauhin.info und dubestemmer.no/en.

---

[52] Auf eine vollständige Diskussion des aktuellen Daten- und Verbraucherschutzes wird im Rahmen der Studie verzichtet.

[53] Siehe z.B. Stellungnahme unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2010/EDPS-2010-12_IMI_DE.pdf

[54] Aussage von Peter Schaar, dem Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) in der Sendung „Kerner" vom 12. August 2010.

[55] https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/TR_RFID/trfid_node.html

Ein Ziel der gesetzlichen Neuerungen könnte zudem sein, dass der Nutzer Eigentümer seiner Daten bleibt und die alleinige Kontrolle über die Datennutzung besitzt. Ob das sinnvoll ist, und wie das umzusetzen wäre, müsste aber erst noch untersucht werden. Die Änderung der automatischen Übertragung sämtlicher Urheberrechte zu einer Datenverwendung dürfte nach Buhl und Müller (2010) nur nach einer ausdrücklichen Einwilligung durch den Benutzer erfolgen, wie das bei Facebook bereits der Fall ist.

3 Offene Fragen

Die technischen Entwicklungen im Bereich der Web 2.0 Dienste, der Kommunikationstechnik sowie auch der in den Markt dringenden Lokalisierungsdienste erfreuen sich großer Beliebtheit bei den Nutzern. Die technischen Möglichkeiten werden oft als vorteilhaft und wünschenswert wahrgenommen. Dabei gibt es wenige Anzeichen dafür, dass die Nutzer die negativen Aspekte, welche vor allem seit Anfang 2010 verstärkt in den Medien diskutiert wurden, so einschätzen, dass sie ihr Verhalten ändern. Das mag zum einen damit zusammenhängen, dass es eben eine notwendige Bedingung ist, Informationen über sich als Nutzer freizugeben, um den Nutzen oben genannter Technologien realisieren zu können. Zum anderen könnte es daran liegen, dass die meisten Nutzer die potentiellen Gefahren, die in den doch zahlreich erschienen Veröffentlichungen zu diesem Thema genannt wurden, für sich individuell anders bewerten, als die Autoren dieser Publikationen. Diese sehen insbesondere potentielle Gefahren für den Datenschutz, die Privatsphäre und die informationelle Selbstbestimmung.

Nimmt man diese Diskrepanz zwischen der von ITA-Experten, Datenschützern und auch verschiedenen Technikexperten konstatierten neuen Qualität der potentiellen Gefahren und dem faktisch beobachteten Verhalten der Nutzer Ernst, so sollte genau diese Diskrepanz die Fragestellung einer empirisch fundierten Technikfolgenabschätzung werden. So wäre zu prüfen, ob die Sensibilität gegenüber den neuen Medien und den modernen Technologien in Bezug auf die Gefahren für die Privatsphäre der Individuen durch eine allgegenwärtige Bereitschaft zu privaten Bekenntnissen gesunken ist. Um die Sicht der Nutzer stärker in die Forschung mit einzubeziehen, veranstaltet z.B. das Zentrum für Technikfolgenabschätzung in Bern (Schweiz, TA SWISS) im November 2010 eine Podiumsdiskussion mit Bürgern, Politikern, Personen aus Verwaltung und Privatwirtschaft sowie Datenschutzspezialisten[56]. Trotz dieses ersten Ansatzes, den Nutzer in den Mittelpunkt von ITA zu stellen, bleibt die Einstellung der Nutzer zu Privatheit und informationeller Selbstbestimmung bei den neuen Diensten und dem globalen Datenaustausch immer noch unklar, so dass die Einstellung der Nutzer zu unterschiedlichen Anwendungszusammenhängen weiter zu analysieren ist.

Da die oben genannten Studien häufig davon ausgehen, es wäre ein mangelndes Wissen seitens der Nutzer zu vermuten, welches zu vergleichsweise sorglosem Umgang mit den Informationstechniken verleite, sollten den Nutzern (beispielsweise von Facebook oder „Wer kennt wen“[57]) zunächst Fragen zu folgenden Themen gestellt werden, um dieser Vermutung nachzugehen:

Welche Kenntnisse haben die Nutzer darüber, für wen Daten sichtbar und zugreifbar sind und wo und wie lange Daten gespeichert werden? Was wissen die Nutzer darüber, zu ermitteln, wer auf ihre Daten zugegriffen hat und in welcher Weise diese Daten weiterverwendet wurden? Ist ihnen bewusst, wem die Daten, die sie ins Netz stellen, gehören (Rannenberg, Kahl, Böttcher 2009)? Ist ihnen bewusst, wem die aus ihren Suchanfragen generierten Datenprofile gehören? Was wissen die Nutzer darüber, ob und wenn ja, wie sie ihre Daten dauerhaft schützen bzw. auch löschen können? Was würden die Nutzer von einer Art „Verfallsdatum oder „digitalem Radiergummi“ halten?

Auf der Basis der Ergebnisse derartiger Interviews könnte die Bereitschaft erhoben werden, welchen technischen, ökonomischen und zeitlichen Aufwand die Nutzer als akzeptabel empfinden, um durch technische Lösungen ihre Privatheit besser zu schützen. Dabei muss immer unterstellt werden, dass durch diese Verfahren auch der maximale Nutzen dieser Informationsdienste vermindert wird. In welchem Ausmaß dieses der Fall ist, müsste zunächst für die verschiedenen technischen Lösungsansätze beurteilt werden. Grundsätzlich wäre somit u.a. **die Nutzerakzeptanz bei technischen und regulatorischen Mechanismen zur Erhöhung des Schutzes der Privatsphäre** abzuklären.

[56] Nähere Informationen unter http://www.ta-swiss.ch/d/them_info_web2.0.html
[57] http://www.wer-kennt-wen.de

Die Analyse technischer Lösungsansätze wie z.B. Privacy Enhancing Technologies (PETs) wäre in Erwägung zu ziehen, um deren Potential zur Abwehr unerwünschter Zugriffe auf und Verkettung von personenbezogenen Daten bestimmen zu können. Wichtige Ansatzpunkte könnten hier auch das Umsetzungs- und Lösungspotential von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungstechnologien sein. Der Einsatz dieser Maßnahmen sollte auf deren Angreifbarkeit durch z.B. sog. De-Anynomisierungstools untersucht werden. Darüber hinaus sollte grundsätzlich evaluiert werden, was für Erfahrungen es mit Verschlüsselungs- und Anonymisierungsdiensten etc. (PET) bereits gibt und wo es sinnvoll wäre, sie einzusetzen. Grundsätzlich wäre beim Einsatz aller Technologien über eine Standardeinstellung und Maßnahmen à la „Schutz der Privatsphäre" nachzudenken. Zudem könnten zusätzliche „Privacy by Design"-Lösungen angedacht werden (vgl. Borcea-Pfitzmann, Pfitzmann, Berg 2011). Die Option einer Datenminimierung, sowohl bei der Erhebung als auch bei der Speicherung, könnte ebenso relevant sein.

Auf der Basis dieser Erhebung könnte diskursiv ein wünschenswerter ‚Grad' des Datenschutzes und der informationellen Selbstbestimmung erhoben werden, der einem Schutzniveau, welches in verschiedenen Studien beschrieben wurde, gegenübergestellt werden könnte.

Gemeinhin konstatieren die Studien, dass neben der Möglichkeit des Wissensaustauschs, der Kommunikation unter Freunden und anderem, soziale Netzwerke nach Ansicht von Datenschützern und Sicherheitsforschern potentiell erhebliche Gefahren für den Datenschutz und die informationelle Selbstbestimmung bergen. Diesbezüglich wäre in speziellen ITA-Studien u.a. zu klären, welche technischen und rechtlichen Anforderungen Netzwerke erfüllen bzw. bieten müssten, um den Datenschutz und die Selbstbestimmung zu maximieren. Daneben wäre zu untersuchen, wie z.B. SNS gestaltet werden müssten, damit Nutzer selbst über den Umgang mit ihren Daten entscheiden können. Diese Fragen könnten in einer Analyse der **Handlungsoptionen zur Verbesserung des Schutzes der Privatsphäre bei neuen Datendiensten** eruiert werden.

Wenn sich herausstellen sollte, dass die Nutzer gerne besser über die potentiellen Gefahren aufgeklärt wären, dann könnte auch die Bewusstseinsbildung der Nutzer, d.h. ein Aufzeigen der möglichen Vor- und Nachteile der Technologien und darüber hinaus das ‚Beibringen' eines verantwortungsvollen Umgangs mit den eigenen Daten, sinnvoll sein. Dabei wäre eine weitere zu klärende Frage, ob Erwachsene grundsätzlich anders mit dem Thema Privatsphäre umgehen als Jugendliche (u.a. Digital Natives) und welchen Einfluss dies auf die Problematik haben könnte. Eine aktive Mitwirkung an der Bewusstseinsbildung und dem Erlernen von sozialer IT-Kompetenz bei Nutzern aus allen Altersgruppen durch Schulen, öffentliche Bildungseinrichtungen, aber evtl. auch Netzwerkbetreibern könnte sich als erstrebenswertes Ziel herausstellen. Von Bedeutung wäre speziell die Ausbildung und Qualifikation der Lehrenden. Neben einer Bewertung bestehender Konzepte wäre die Erarbeitung eines Konzepts mit **Maßnahmen zur Bewusstseinsbildung bei neuen Datendiensten** empfehlenswert, ggf. auch in Kombination mit Maßnahmen zur Verbesserung bzw. Erweiterung des technischen Know-hows und dessen Anwendung.

Über Lokalisierungsdienste ergeben sich zusätzliche Möglichkeiten einer umfassenden Profilerstellung bzgl. der Interessen sowie der Verbrauchs- und Bewegungsgewohnheiten von Privatpersonen. Ungeklärt ist noch, ob sich der Staat, Unternehmen oder Einzelpersonen durch das Nutzen von Lokalisierungsdiensten oder dem Sammeln und Verketten von Internet-Profilen Überwachungs-, Mobbing- oder Manipulationsmöglichkeiten verschaffen könnten. Hierbei ist auch an die Übermittlung von Funknetzdaten in die USA durch Google und Apple und schließlich durch Verschiebung personenbezogener Daten im Rahmen der Auslagerung von EDV-Prozessen ins Ausland zu denken (Cloud Computing). Dabei wäre grundlegend zu ermitteln, welche Verkettungsmöglichkeiten von – freiwillig in SNS zur Verfügung gestellten und bei Rechercheanfragen generierten – Daten mit anderen Datenbeständen bestehen, wer die Daten zu Persönlichkeitsprofilen verkettet und evtl. verkauft, für welchen Zweck sie verwendet werden und ob dies rechtlich zulässig ist bzw. wie dies bei ausländischen Akteuren kontrolliert werden kann. Es wird auch diskutiert, ob

die Untersuchung und ggf. Überarbeitung der Filterregeln von Suchmaschinen, die beispielsweise dazu führen könnte, dass Suchmaschinen den selbst in das Netz gestellten Daten höhere Priorität einräumen als fremd erzeugten Daten oder Profilen, eine sinnvolle Maßnahme ist (de Maizière 2010). Generell wäre eine **Untersuchung zur Nutzung, Verkettbarkeit und Weiterverwendung von Daten bzw. Persönlichkeitsprofilen** sinnvoll[58]. Ein Ergebnis dieser Abwägung bzw. Analyse könnten u.a. verbindliche Regularien sein, die Missbrauch bestrafen und im besten Fall unterbinden.

Parallel könnte analysiert werden, welches **globale Potential die Nutzung anonymer Kommunikationsdienste** z.B. in undemokratischen Staaten für Demokratisierungsprozesse und die Entwicklung dieser Länder haben könnte. Dabei wäre darauf zu achten, ob die vorhandene Kommunikationstechnik in diesen Ländern eine anonyme oder eine Nutzung durch „Tunnel“ und Anonymisierungsdienste erlaubt.

Darüber hinaus wäre grundsätzlich zu klären, welche **Sicherheitslücken von Endgeräten** bestehen könnten. Ein Schutz privater Daten ist grundsätzlich nur einzuhalten, wenn die Endgeräte eine entsprechende Kontrolle erlauben. Dies betrifft Bereiche, wie das Gesundheitswesen und die Verschlüsselung von Daten auf dem Transport, wie auch allgemein die Geheimhaltung von Login-Informationen. Phishing (password fishing) aus dem Bereich Homebanking, genauso wie Wirtschaftsspionage zeigen nach einem Bericht von Symantec (2009), dass die Endgeräte bisher nicht sicher genug sind. Der Bedarf, diese Sicherheitslücken zu untersuchen, ergibt sich aus der nahezu alltäglichen Notwendigkeit mit einem Endgerät ins Netz gehen zu müssen. Ein Gesichtspunkt wäre dabei die Klarstellung, ob die aktuellen Techniken ausreichend gegen Missbrauch geschützt werden können. Dabei sollte ein besonderer Augenmerk auf die erforderlichen technischen Innovationen gelegt werden, die Endgeräte ‚sicher(er)’ machen.

[58] Staatssekretär Max Stadler schlug nach einem Spiegel-Artikel vom 6. September 2010 vor, professionellen Datensammlern, die mit dem Material komplette Bewegungsprofile erstellen können, das Leben schwerer zu machen und entsprechende Daten mit einem Verfallsdatum zu versehen. Siehe http://www.spiegel.de/netzwelt/web/0,1518,715878,00.html

4 Vorschläge zur methodischen Umsetzung

Die Chancen und Risiken moderner Kommunikation, von Web-2.0-Diensten und allgegenwärtiger Datenverarbeitung werden sowohl in der Öffentlichkeit wie auch auf wissenschaftlicher Ebene breit diskutiert. Fragen zu Datenschutz, Privatsphäre und informationeller Selbstbestimmung in der ‚digitalen Welt' waren bereits in zahlreichen Studien Untersuchungsgegenstand. Allerdings gibt es einen Mangel an Vorschlägen zur Umsetzung konkreter technischer und juristischer Handlungsoptionen, die sich auf die neuen Dienste beziehen. Die offenen Fragen (s. Kapitel 3, S. 29) legen den Schluss nahe, dass solche technischen und juristischen Maßnahmen noch kaum festgelegt werden können, da noch zu wenig Wissen über die faktische Einschätzung der Nutzer dieser potentiellen Risiken bekannt ist. Gleichermaßen sind Chancen und Optionen technischer Möglichkeiten, jenseits der neuen Dienste zur Verbesserung des Schutzes der Privatsphäre zu prüfen. Demnach würden die im Folgenden beschriebenen und in vier Cluster eingeteilten, denkbaren ITA-Aktivitäten in Bezug auf die potentiellen Chancen und Risiken der Techniken bereits verfasste Studien einbeziehen, den Fokus aber auf die Beurteilung dieser Gefahren und der Chancen von Optionen durch die Nutzer legen.

1. Untersuchung zur Nutzung, Verkettbarkeit und Weiterverwendung von Daten

Gegenstand: Hierbei geht es um die Nutzung von Daten durch Betreiber und deren Weitergabe, sowie um die Sekundärauswertung von Daten aus dem WWW durch weitere Akteure. Insbesondere soll der Umgang von Suchmaschinenbetreibern (Algorithmen, Beeinflussbarkeit, Sekundärnutzung), LBS-Betreibern, SNS-Anbietern, Handyherstellern (wie Apple), NFC-Betreibern und Banken, Cloud Computing-Betreibern, etc. mit Daten untersucht werden. Es sollten u.a. Themen, wie die Kontrolle und das Eigentum an den Daten, ausgeübt durch Individuen und lokale Unternehmen (bspw. Firmen, die Cloud Computing nutzen, in- und ausländische Behörden), untersucht werden. Auch hier steht die Ambivalenz der Technik im Zentrum. Verkettung und sekundäre Auswertung können gleichermaßen zum Schaden wie zum Vorteil der Nutzer eingesetzt werden.

Umsetzung: Experten- und Interessenvertreter-Interviews; Recherche des Status Quo der technischen Möglichkeiten, potentieller Entwicklungen und ihrer Grenzen; Dialog-Prozess zu Gestaltungs- und Regulierungsfragen.

2. Der Nutzer im Fokus von ITA

2a. Einstellung der Nutzer zu Privatheit und informationeller Selbstbestimmung bei neuen Datendiensten

Nach wie vor scheint das Thema Datensicherheit und digitale Identität in einem Spannungsverhältnis zwischen wissenschaftlichem Problembewusstsein auf Seiten vieler Experten und Vertreter demokratischer Institutionen und dem scheinbar diesem nicht entsprechenden Nutzungsverhalten bei Online-Diensten zu stehen.

Gegenstand: Nutzer geben zunehmend bei elektronischen Diensten private Daten preis. Hier wird an Dienste wie Social Networking Services, Location Based Services, drahtlose Kommunikation (insb. Verbindungsdaten), online verfügbare Anwendungen oder Suchdienste gedacht. Die Einstellung der Nutzer zu Privatheit und informationeller Selbstbestimmung in der digitalen Welt ist dabei aber unklar, wie auch, ob sich die Nutzer bewusst sind, was mit ihren Daten passiert und inwieweit datenschutzrechtliche Regulierungen angemessen sind und auf Akzeptanz treffen.

Die Antworten auf die im vorherigen Kapitel explizit formulierten Fragen werden Aufschluss darüber bringen, ob es sich um bewusst eingegangene Risiken handelt, um auf Nicht-Wissen basierendes ‚Fehl'-

Verhalten oder ob neue Formen von Techniknutzung und des Schutzes der Privatsphäre gesucht werden sollten.

Umsetzung: Evaluierung des Nutzerverhaltens z.B. durch Interviews, um eine individuelle Einschätzung der Argumentationsmuster erkennen zu können; Fokusgruppen, um diskursiv auf der Basis der Argumentationsmuster die genaueren Argumentationszusammenhänge ermitteln zu können; ggf. eine repräsentative Umfrage unter Nutzern unter Zuhilfenahme der Argumentationsmuster.

2b. Handlungsoptionen zur Verbesserung des Schutzes der Privatsphäre bei neuen Datendiensten

Gegenstand: Es sollte erhoben werden, welche Optionen es für einen höheren Schutz der Privatsphäre gibt (technische, regulatorische, freiwillige). Darüber hinaus sollte beleuchtet werden, ob Nutzer stärkere Rechte bezüglich der Weiterverwendung, des Löschens und der Veränderung von Daten erhalten wollen und sollten. Angesichts anstehender regulatorischer Aktionen in der EU (Datenschutzbeauftragter Hustinx) und in den USA (National Strategy for Trusted Identities in Cyperspace) wäre die Herausarbeitung von Optionen sinnvoll, die die Ziele der Nutzer und Betreiber aufgreifen und innovativ berücksichtigen.

Umsetzung: Durch die enge Verwobenheit der technischen Umsetzbarkeit und der wünschenswerten Privatheit könnte eine Bürgerjury eine sinnvolle Methode sein. Experten erläutern hierbei vor einer Jury aus Bürgern die Möglichkeiten und Grenzen der verschiedenen technischen Optionen. Die Jury bewertet dann die unterschiedlichen Lösungen. Ergebnis einer Bürgerjury könnte beispielsweise die Festlegung eines ‚Datenschutzniveaus' sein. So werden Nutzer, Anbieter und Experten involviert. Ein weiteres votensuchendes Verfahren könnte eine Konsensuskonferenz sein, bei der Dissense und Konsense mit den jeweiligen Begründungen gehört würden. Dazugehörige Dialogprozesse sollten zumindest die EU und die USA einbeziehen.

2c. Nutzerakzeptanz bei technischen und regulatorischen Mechanismen zur Erhöhung des Schutzes der Privatsphäre

Gegenstand: Ausgehend von den Ergebnissen der Projekte 1., 2a. und 2b. sollte im Bereich technischer Möglichkeiten zur Verbesserung des Datenschutzes zunächst eine Bestandsaufnahme über praxisrelevante und bereits realisierte und realisierbare Lösungsansätze zur Verringerung der Anzahl personenbezogener Daten und Verbesserung des Schutzes gespeicherter Daten sowie deren Anwenderfreundlichkeit erfolgen. Es gilt zu untersuchen, welches die Voraussetzungen sind, damit diese Instrumente dem Anwender vertraut gemacht werden können. Fragen der anwenderfreundlichen Implementierung von datenschutzbezogenen „Brandmauern" oder Zertifizierung von datenschutzkonformen Web 2.0-Diensten könnten hier u.a. eine Rolle spielen.

Darüber hinaus scheint auf Nutzerseite die Funktionsweise verschiedener technischer Datenschutzmechanismen kaum bekannt zu sein. Die Vor- und Nachteile derartiger Maßnahmen können nur schwer eingeschätzt werden, und ein möglicher Verlust von Anwenderfreundlichkeit könnte die Nutzer abschrecken. Vor diesem Hintergrund müssten die technischen Möglichkeiten des Datenschutzes einer nutzerorientierten Evaluation unterzogen werden.

Umsetzung: Zunächst könnten in Workshops mit Experten und Nutzern bestehende und potentielle Handlungsoptionen herausgearbeitet und diese bewertet werden. Daneben könnten Modellversuche mit Nutzern Aufschluss darüber liefern, welche technischen Mechanismen des Datenschutzes von den Nutzern akzeptiert werden und damit geeignet sind, in der Praxis Anwendung zu finden. Kriterien hierfür könnten die ‚Größe' eines möglichen Performanz-Verlustes des technischen Dienstes sein, die eventuell anfallenden Kosten, die für diese Mechanismen aufgewendet werden müssen, oder der in Betracht kommende zusätzli-

che Zeitaufwand, der seitens der Nutzer erbracht werden muss, aber ggf. natürlich auch die potentiell Zeitersparnis oder die größere Freiheit bei anonymen oder pseudonymen Nutzungen. Diese Kriterien sind in Modellversuchen zu entwickeln. Außerdem könnte mit ITA-Projekten zu „Privacy-by-Design", die anbieterorientierten technischen Möglichkeiten des Datenschutzes näher beleuchtet werden. Es sollte hierbei die Frage geklärt werden, welche Datenschutzmechanismen die Dienstanbieter für akzeptabel bzw. sogar wünschenswert halten. Hierbei kann es vor allem darum gehen, Anbieter- und Anwenderinteressen zu vergleichen, konsensfähige Optionen des Datenschutzes zu erarbeiten, und dessen Umsetzung zu begleiten. Vor allem vor dem Hintergrund unterschiedlicher Geschäftsmodelle auf Anbieterseite ist diese Fragestellung zentral.

2d. Maßnahmen zur Bewusstseinsbildung bei neuen Datendiensten

Gegenstand: Unter Berücksichtigung der Ergebnisse der fortschreibenden ITA-Projekte 2a. bis 2c. sollten bestehende Maßnahmen zur Bewusstseinbildung auf ihre Adäquatheit überprüft werden. Zudem wäre zu untersuchen, ob eine aktive Mitwirkung an der Bewusstseinsbildung durch Schulen, öffentliche Bildungseinrichtungen, aber evtl. auch Netzwerkbetreiber in Erwägung gezogen werden sollte. Hier könnte u.a. über das Integrieren von Lernmodulen zur Erhöhung sozialer IT-Kompetenz in den Lehrplan von Schulen nachgedacht werden.

Umsetzung: Evaluierung von Maßnahmen zur Meinungs- und Bewusstseinsbildung (wie z.B. http://www.schau-hin.info); Neu- und Weiterentwicklung von bewusstseinsbildenden Maßnahmen, bspw. in Bezug auf Erwachsene; Sekundärauswertung von Daten.

3. Globales Potential der Nutzung anonymer Kommunikationsdienste

Gegenstand: Anonyme Kommunikationsdienste und ihr globales Potential sollten aus mehreren Gründen untersucht werden. Sie könnten u.a. in undemokratischen Ländern in Demokratisierungsprozessen genutzt werden, womit letztlich Frieden und Entwicklung dieser Länder gefördert und mitunter auch Dumpinglöhnen entgegengewirkt werden würde. Dabei wäre darauf zu achten, dass vorhandene Kommunikationstechnik in diesen Ländern entweder eine anonyme Nutzung oder eine Nutzung durch „Tunnel" und Anonymisierungsdienste erlaubt (auch Pseudonyme, auch drahtlose Netze). D.h. die zunehmende Verbreitung des Internets bietet hier Chancen. Dabei wäre es wichtig, dass Systeme und Endgeräte in den Herstellerländern bereits so gestaltet werden, dass die Nutzer Dienste zur Herstellung unverkettbarer Kommunikation nutzen können. Dies erfordert ggf. politische Prozesse und einen globalen Diskurs um die möglichen Vor- aber auch potentielle Nachteile (Missbrauchsrisiken). Aber auch in demokratischen und demokratisierten Staatswesen spielt die anonymisierte Kommunikation im Internet eine zunehmend wichtige Rolle. Hierbei stellt sich v.a. die Frage, inwieweit Anonymisierung und Pseudonymisierung von informationeller Urheberschaft zu einem Wandel von politischer Öffentlichkeit und gesellschaftlichen Kommunikationsprozessen führen.

Zu den nachteiligen Folgen einer verstärkten Verbreiterung von Anonymisierungsdiensten im Internet gehört die Erschwernis von Strafverfolgung durch staatliche Behörden. Insofern steht die Forderung nach einfachen und weitreichenden Anonymisierungsmöglichkeiten in den IKT mit den Forderungen von Strafverfolgungsbehörden nach Möglichkeiten der Verbesserung der Strafverfolgung im Internet in einem ständigen Spannungsverhältnis. Für die erfolgreiche Verfolgung von Straftaten im Internet wäre eine weitreichende Aufhebung von Anonymisierungsvorgängen erforderlich. Die globale Perspektive jedoch – einige Anonymisierungsdienste machen sich die unterschiedliche Rechtslage in verschiedenen Staaten zunutze – verstärkt diese Problematik.

Die deutsche Industrie könnte in einem globalen Wachstumsmarkt der Anonymisierungstechnologien eine besondere Rolle in der Lieferung von Komponenten zur anonymen Kommunikation einnehmen. Darüber hinaus wäre das Potential pseudonymer, anonymer und unverkettbarer Dienste im Inland zu untersuchen (Suchdienste, LBS, SNS, Wahlen etc.).

Umsetzung: Das Feld wäre zunächst zu explorieren. Veranstaltungen, Blogs etc. könnten zur Herausarbeitung sinnvoller Optionen führen.

4. Endgerätesicherheit

Gegenstand: In einem offenen Netz wie dem Internet ist weiter mit der Verbreitung von Schadcode zu rechnen, der den Diebstahl oder die Manipulation privater Daten zum Ziel hat (Homebanking, Wirtschaftsspionage, Sabotage etc.). Als Gegenmaßnahmen stehen grundsätzlich folgende Optionen zur Verfügung: Separate, sichere Hardware mit Nutzer-Input und -Output, die Verbesserung von üblichen Betriebssystemen und der Einsatz von Virtualisierung zur Isolierung von Schadcode (als quelloffen oder -geschlossen).

Umsetzung: Analyse, ob Lösungen am Markt entstehen; Analyse staatlicher Fördermaßnahmen (etwa Spezifikationen im Beschaffungswesen); Dialog-Prozesse.

5 Weiterführende Literatur

Bizer, J.; Dingel, K.; Fabian,B.; Günther, O.; Hansen, M.; Klafft, M.; Möller, J.; Spiekermann, S. (2006)*:* TAUCIS – Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung. Studie im Auftrag des BMBF. Berlin. http://www.bmbf.de/pub/ita_taucis.pdf; abgerufen am 22.06.2010

Čas, J. (2008): Datenschutz bei Pervasive Computing im Gesundheitswesen. In: Technikfolgenabschätzung – Theorie und Praxis 17(1) (2008), S. 57-65

European Technology Assessment Group (2007): RFID and Identity Management in Everyday Life. Striking the balance between convenience, choice and control. STOA 2006-22. http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf, abgerufen am 21.06.2010

Friedewald M.; Raabe, O.; Koch, D. J.; Georgieff, P.; Neuhäusler, P. (2009): Zukunftsreport - Ubiquitäres Computing. Studie des Büros für Technikfolgenabschätzung beim Deutschen Bundestag. Arbeitsbericht Nr. 131. Mai 2009, http://dip21.bundestag.de/dip21/btd/17/004/1700405.pdf; abgerufen am 21.06.2010

Friedewald M. et al. (2009): Privacy and Trust in the Ubiquitous Information Society: Analysis of the impact of convergent and pervasive ICT on privacy and data protection and needs and options for development of the legal framework. Final Report for the European Commission. Karlsruhe

Gabriel, P.; Bovenschulte, M.; Hartmann, E.; Groß, W.; Strese, H.; Bayarou, K.; Haisch, M.; Mattheß, M.; Brune, C.; Strauss, H. et al. (2006): Pervasive Computing – Entwicklungen und Auswirkungen (PerCEntA). Studie des Bundesamtes für Sicherheit in der Informationstechnik in Kooperation von VDI/VDE Innovation und Technik GmbH. Fraunhofer Institut für sichere Informationstechnologie und Sun Microsystems GmbH. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Percenta/Percenta_dlay_pdf.pdf?__blob=publicationFile; abgerufen am 18.04.2011

Heatherly, R.; Kantarcioglu, M.; Thuraisingham, B.; Lindamood, J. (2009): Preventing Private Information Inference Attacks on Social Network., Technical Report University of Texas at Dallas. UTDCS-03-09, verfügbar unter http://www.utdallas.edu/~mxk055100/publications/UTDCS-03-09-fb-anon.pdf; abgerufen am 21.06.2010

Hilty, L. M.; Behrendt, S.; Binswanger, M.; Bruinink, A.; Erdmann, L.; Fröhlich, J.; Köhler, A.; Kuster, N.; Som, C.; Würtenberger,F. (2003): Das Vorsorgeprinzip in der Informationsgesellschaft. Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. TA 46/2003. Bern, http://www.ta-swiss.ch/d/arch_info_perv.html; abgerufen am 21.06.2010

van't Hof, C.; Cornelissen, J. (2006): RFID and Identity Management in Everyday Life. Case Studies on the Frontline of Developments towards Ambient Intelligence. Deliverable No. 2 of the project RFID and Identity Management. Commissioned by STOA and carried out by ETAG, http:// www.itas.fzk.de/eng/etag/document/hoco06a.pdf; abgerufen am 22.06.2010

van Lieshout, M.; Grossi, L.; Spinelli, G.; Helmus, S.; Kool, L.; Pennings, L.; Stap, R.; Veugen, T.; van der Waaij, B.; Borean, C. (2007): RFID Technologies: Emerging Issues. Challenges and Policy Options. http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1476; abgerufen am 21.06.2010

Oertel, B.; Wölk, M.; Hilty, L. M.; Köhler, A.; Kelter, H.; Ullmann, M.; Wittmann, S. (2004): Risiken und Chancen des Einsatzes von RFID-Systemen, Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in einer interdisziplinären Kooperation vom IZT – Institut für Zukunftsstudien und Technologiebewertung und der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA); verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/RFID/RIKCHA_pdf.pdf?__blob=publicationFile; abgerufen am 18.04.2011

Sterbik-Lamina, J.; Peissl, W.; Čas, J. (2009): Privatsphäre 2.0 – Beeinträchtigung der Privatsphäre in Österreich. TA-Studie der Österreichischen Akademie der Wissenschaften (ÖAW) und des Instituts für Technikfolgenabschätzung (ITA). http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a53.pdf; abgerufen am 17.07.2010

VDI/VDE Innovation + Technik GmbH (2007): RFID – Potenziale für Deutschland, Stand und Perspektiven von Anwendungen auf Basis der Radiofrequenz - Identifikation auf den nationalen und internationalen Märkten. Studie für das Bundesministerium für Wirtschaft und Technologie (BMWI), http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/rfid-potenziale-fuer-deutschland,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf; abgerufen am 18.04.2011

6 Literaturverzeichnis

Aarts, E.; Marzano S. (Hg.) (2003): The New Everyday: Views on Ambient Intelligence. 010 Publishers. Rotterdam

Acquisti, A.; Grossklags, J. (2005): Privacy and Rationality in Individual Decision Making. In: IEEE Security and Privacy 3(1) (2005), S. 26-33

Acquisti, A., Gross, R. (2006): Imagined communities: Awareness, information sharing, and privacy on the Facebook. In: Golle, P.; Danezis G. (Hg.): Proceedings of 6th Workshop on Privacy Enhancing Technologies, Cambridge, S. 36-58

Adamowsky, N. (2010): Medialisierte Umgebungen und Strategien der Kontingenzbewältigung. Digitale Überwachungssysteme im Modus des Spiels. In: Münkler, H.; Bohlender M.; Meurer, S. (Hg.): Sicherheit und Risiko. Bielefeld, S. 223-238

Albrecht, K.; McIntyre, L. (2005): Spychips: How Major Corporations and Government Plan to Track Every Move with RFID. Nelson Current. Nashville

Al-Kassab, J.; Blome, J.P.; Wolfram, G.; Thiesse, F.; Fleisch, E. (2010): RFID in the Apparel Retail Industry: A Case Study from Galeria Kaufhof. In: Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks. Berlin, S. 281-308

Anderson, A. M.; Labay, V. (2006): Ethical considerations and proposed guidelines for the use of radio frequency identification. Especially concerning its use for promoting public safety and national security, In: Science and Engineering Ethics 12(2) (2006), S. 265-272

Art (2010): Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising. 00909/10/EN. WP171. Brüssel. verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf; abgerufen am 13.09.2010

Arte (2008): Anonymität im Internet – Ist Privatsphäre möglich?! Arte Dokumentarfilm. ausgestrahlt am 12.07.2008

Baghdassarian, S.; Milanesi, C. (2009): Dataquest Insight: Applications Stores; The Revenue Opportunity Beyond the Hype. Gartner Inc.

Barnes, S. B. (2006): A privacy paradox: Social networking in the United States. In: First Monday 11(9) (2006); verfügbar unter http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312#b1; abgerufen am 8.September 2007

Becker, S. (2010): Wie Bürger ihre Daten schützen können – Forschungsprojekt für zu Prototyp für eine bessere informationelle Selbstbestimmung. In: Informationsdienst Wissenschaft. Pressemitteilung vom 14.10.2010

Beckwith R. (2003): Designing for Ubiquity: The Perception of Privacy. In: IEEE Pervasive Computing 2(2) (2003), S. 40-46

Bick, M; Kummer, T.-F.; Rössig, W. (2008): Ambient Intelligence in Medical Environment and Devices – Qualitative Studie zu Nutzerpotentialen ambienter Technologien in Krankenhäusern. ESCP-EAP Working Paper 36. Berlin; http://www.escp-eap.eu/uploads/media/AIMED_04.pdf

Billich, C. (2007): Mobile Japan 2007. Tokyo; www.infinita.co.jp/Infinita_Mobile_Japan_2007.pdf

Bizer, J.; Dingel, K.; Fabian, B.; Günther, O.; Hansen, M.; Klafft, M.; Möller, J.; Spiekermann, S. (2006): TAUCIS – Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung. Studie im Auftrag des BMBF. Berlin; http://www.bmbf.de/pub/ita_taucis.pdf; abgerufen am 22.06.2010

Bizer, J. (2007): Modernisierung des Datenschutzes: 4 Säulen des Datenschutzes. Stellungnahme des ULD zur Anhörung des Innenausschusses des Deutschen Bundestages „Modernisierung des Datenschutzes“ am 5. März 2007. In: Datenschutz und Datensicherheit 31/2007, S. 264-266

BMI (Bundesministerium des Inneren) (2010a): Elektronischer Reiseausweis. Berlin; verfügbar unter http://www.epass.de/; abgerufen am 21.07.2010

BMI (Bundesministerium des Inneren) (2010b): Alles Wissenswerte zum neuen Personalausweis. Berlin; verfügbar unter http://www.bmi.bund.de/cln_165/SharedDocs/Downlads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/broschuere_neuer_perso2.html; abgerufen am 26.08.2010

Borcea-Pfitzmann, K.; Pfitzmann, A.;Berg, M. (2011): Privacy 3.0 := Data Minimization + User Control + Contextual Integrity. In: Information Technology (IT) Vol. 52 (1). S. 34-40

Borchers, C. M. (2008): Die Einführung der elektronischen Gesundheitskarte in das Deutsche Gesundheitswesen - Datenschutzrechtliche Probleme und Gefahren strafrechtlich relevanten Missbrauchs. In: Hilgendorf, E. (Hg.): Das Strafrecht vor neuen Herausforderungen (Bd.12).Würzburg, S. 94-110

Boyd, D.; Ellison, N. E. (2007): Social networking sites: Definition, history and scholarship. In: Journal of Computer-Mediated Communication Vol. 13(1) (2007), S. 210-230; verfügbar unter http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Buhl, H. U.; Müller, G. (2010): Der gläserne Bürger im Web 2.0. Herausforderungen des „virtuellen Striptease". In: Wirtschaftsinformatik 52(4) (2010), S. 193-197

Cameron, K. (2009): The Laws of Identity - Microsoft: minimum disclosure about minimum disclosure?; verfügbar unter http://www.identityblog.com/?p=1066, abgerufen am 01.10.2010

Čas, J. (2008): Datenschutz bei Pervasive Computing im Gesundheitswesen. In: Technikfolgenabschätzung – Theorie und Praxis 17(1) (2008), S. 57-65

Čas, J.; Peissl, W. (2010): Datenhandel – ein Geschäft wie jedes andere?. Bundeszentrale für politische Bildung. Spezial: Wissen und Eigentum; http://www.bpb.de/themen/JX32Z9,0,Datenhandel_%96_ein_Gesch%E4ft_wie_jedes_andere.html veröffentlich am 15. März 2010

Cavoukian, A. (2010): Sensors and In-Home Collection of Health Data: A Privacy by Design Approach. Intelligent Assistive Technology & Systems Lab and Information & Privacy Commissioner. Ontario; verfügbar unter http://www.ipc.on.ca/images/Resources/pbd-sensor-in-home.pdf

Chaum, D. (1992): Achieving Electronic Privacy. In: Scientific American August 1992, S. 96-101

COMM (Commission of the European Communities) (2009): Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection in applications supported by radio-frequency identification, Brüssel, 12.5.2009; http://ec.europa.eu/information_society/policy/rfid/documents/recommendationon rfid2009.pdf

Cyganski, P.; Hass, B. H. (2008): Potenziale sozialer Netzwerke für Unternehmen. In: Hass, B. H.; Walsh, G.; Kilian, T. (2008): Web 2.0. Neue Perspektiven für Marketing und Medien, Berlin/ Heidelberg, S. 101-120

Das, R.; Harrop, P. (2010): RFID Forecasts, Player and Opportunities 2011-2021. IDTechEx

DHS (Department of Homeland Security) (2010): National Strategy for Trusted Identities in Cyperspace. Washington; verfügbar unter http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

Dix, A. (2009): Informations- und datenschutzrechtliche Aspekte von Ambient Assisted Living Technologies – Was muss man beachten? Ambient Assisted Living: 2 Deutscher Kongress mit Ausstellung. Technologie – Anwendungen – Management. 27.–28. Januar 2009. Tagungsband. Berlin

Dobson, J. E.; Fisher, P. F. (2003): Geoslavery. In: IEEE Technology and Society Magazine 22(1) (2003), S. 47-52

Dobson, J. E. (2009): Big Brother has evolved. In: Nature 458 (968) (2009); http://www.nature.com/nature/journal/v458/n7241/full/458968a.html

Dritsas, S.; Tsaparas, J.; Gritzalis, D. (2006): A Generic Privacy Enhancing Technology for Pervasive Computing Environments. In: Fischer et al. (Hg.) (2006): Trust and Privacy in Digital Business. Lecture Notes in Computer Science (Bd. 4083). Berlin/ Heidelberg, S. 103-113

Dwyer, C.; Hiltz, S. R.; Passerini, K. (2007): Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. Proceedings of AMCIS. Keystone, Colorado

ENISA (European Network and Information Security Agency) (2010a): Online as soon as it happens. Positionspapier. Februar 2010; verfügbar unter http://www.enisa.europa.eu/act/ar/deliverables/2010/online asithappens/at_download/fullReport

ENISA (European Network and Information Security Agency) (2010b): Mobile Identity Management. Positionspapier. April 2010; verfügbar unter http://www.enisa.europa.eu/act/it/eid/Mobile%20IDM/at_download/full Report

ENISA (European Network and Information Security Agency) (2010c): Industry Proposal for a Privacy Impact Assessment Framework for RFID Applications. Positionspapier. Juli 2010; verfügbar unter http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia

EPoS (European Technology Plattform on Smart Systems Integration) (2008): Internet of Things 2020: Roadmap for the Future. Brüssel; verfügbar unter http://old.smart-systems-integration.org/internet-of-things/ Internet-of-Things_in_2020_ECEPoSS_Workshop_Report_2008_v3.pdf/download

Euro (Europäische Kommission) (2007): Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen. COM (2007) 96. Brüssel; verfügbar unter http://www.epcglobal.ch/down loads/rfid_de.pdf

Euro (Europäische Kommission) (2010): A comprehensive approach on personal data protection in the European Union. COM (2010) 609/3. Brüssel; S. 3-4; verfügbar unter http://ec.europa.eu/justice/news/consulting _public/0006/com_2010_609_en.pdf

FAZ (2010): Privatsphäre muss gewahrt bleiben. In: FAZ.NET. Artikel veröffentlicht am 12.08.2010; verfügbar unter http://www.faz.net/s/Rub594835B672714A1DB1A121534F010EE1/Doc~E6ACFB829E6B145F69 E8F839BCF282B6A~ATpl~Ecommon~Scontent.html

Fleisch, E.; Christ, O.; Dierkes, M. (2005): Die betriebswirtschaftliche Vision des Internets der Dinge. In: Fleisch; E.; Mattern, F. (Hg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. Berlin/ Heidelberg, S. 3-38

Frame (2011): Privacy and Data Impact Protection Assessment Framework for RFID Implications. 12.01.2011, verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf, abgerufen am 18.04.2011

Fransen, J. (2010): Umsatzsprünge von RFID nicht absehbar. Interview mit dem Gründer des Unternehmen Euro I.D. Identifikationssysteme. Interview verfügbar unter http://www.marktplatz-rfid-im-blick.de/201008042183/euro-id-identifikationssysteme-umsatz spruenge-der-rfid-technologie-erst-in-mehreren-jahren-erwartet.html, August 2010, abgerufen am 09.08.2010

Fraunhofer (Fraunhofer-Institut Sichere Informationstechnologie) (2008): Privatsphärenschutz in Soziale Netzwerke-Plattformen. Endbericht. Darmstadt; verfügbar unter http://www.sit.fraun-hofer.de/pressedownloads/ pressemitteilungen/20080925StudieSozialeNetzwerke.jsp; abgerufen am 01.07.2010

Friedewald, M.; Lindner, R. (2008): Gesellschaftliche Herausforderungen durch intelligente Umgebungen: Eine Szenarioanalyse. In: Technikfolgenabschätzung – Theorie und Praxis 17(1) (2008), S. 78-83

Friedewald, M.; Raabe, O.; Koch, D. J.; Georgieff, P.; Neuhäusler, P. (2009a): Zukunftsreport - Ubiquitäres Computing. Studie des Büros für Technikfolgenabschätzung beim Deutschen Bundestag. Arbeitsbericht Nr. 131. Berlin

Friedewald, M.; Leimbach, T.; Wright, D.; Gutwirth, S.; De Hert, P.; Gonzáles Fuster, G.; Langheinrich, M.; Ion, J. (2009b): Privacy and Trust in the Ubiquitous Information Society: Analysis of the impact of convergent and pervasive ICT on privacy and data protection and needs and options for development of the legal framework. Final Report for the European Commission, Karlsruhe; verfügbar unter http://isi.fraunhofer.de/ isi-de/publ/download/isi09b52/Privacy-and-Trust-Ubiquitous-Information-Society.pdf?pathAlias= /publ/downloads/isi09b52/Privacy-and-Trust-Ubiquitous-Information-Society.pdf; abgerufen am 07.07.2010

Gabriel, P.; Bovenschulte, M.; Hartmann, E.; Groß, W.; Strese, H.; Bayarou, K.; Haisch, M.; Mattheß, M.; Brune, C.; Strauss, H. et al. (2006): Pervasive Computing – Entwicklungen und Auswirkungen. Studie des Bundesamtes für Sicherheit in der Informationstechnik in Kooperation von VDI/VDE Innovation und Technik GmbH, Fraunhofer Institut für sichere Informationstechnologie und Sun Microsystems GmbH. Bonn; verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Percenta/Percenta_dlay_pdf.pdf?__blob=publicationFile; abgerufen am 18.04.2011

Gaßner, K.; M. Conrad, M. (2010): ICT enabled independent living for elderly. A status-quo analysis on products and the research landscape in the field of Ambient Assisted Living (AAL) in EU-27. VDI/VDE Innovation und Technik GmbH. Studie für die Europäische Kommission, DG Information Society and Media, ICT for Health Unit, Berlin, März 2010; http://www.aal-deutschland.de/deutschland/dokumente/ict_for_elderly_webversion.pdf

Gibson, B.; W. Holden, W. (2010): Mobile Location Based Services – Applications, Forecasts & Opportunities 2010 – 2014. Juniper Research

Glob (Global Industry Analysts Inc.) (2010): Location Based Services. Report. August 2010

Gross, R.; Acquisti, A. (2005): Information revelation and privacy in online social networks. In: Proceedings of WPES'05, S. 71-80

Gundermann, L. (2008): Telematikinfrastruktur der elektronischen Gesundheitskarte: Basis für sichere Datenspeicherung. In: Deutsches Ärzteblatt 105(6) (2008), S. 268-271

Hansen, M.; Berlich, P.; Camenisch, J.; Clauß, S.; Pfitzmann, A.; Waidner, M. (2004): Privacy Enhancing Identity Management. In: Information Security Technical Report 9(1), S. 35-44

Hansen, M.; Meissner. S. (Hg.) (2007): Verkettung digitaler Identitäten, Ergebnisbericht des Projekts „Verkettung digitaler Identitäten". Berlin; verfügbar unter: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf

Heatherly, R.; Kantarcioglu, M.; Thuraisingham, B.; Lindamood, J. (2009): Preventing Private Information Inference Attacks on Social Networks. Technical Report University of Texas at Dallas. UTDCS-03-09; verfügbar unter http://www.utdallas.edu/~mxk055100/publications/UTDCS-03-09-fb-anon.pdf; abgerufen am 21.06.2010

Heesen, J.; Simoneit, O. (2007): Opportunities for privacy and trust in the development of ubiquitous computing. In: International Review of Information Ethics Vol. 8 (12/2007), S. 48-52

Heidemann, J. (2009): Online Social Networks – Ein sozialer und technischer Überblick, in: Informatik-Spektrum 33(3) (Juli 2009), S. 260-271

Heise (Heise online) (2010): EU-Datenschützer fordert Einbau von Datenschutz in die Technik. Artikel vom 22.03.2010; verfügbar unter http://www.heise.de/newsticker/meldung/EU-Datenschuetzer-fordert-Einbau-von-Datenschutz-in-die-Technik-960735.html; abgerufen am 25.09.2010

Hennig, J. E.; Ladkin, P. B.; Sieker, B. (2004): Privacy Enhancing Concepts for RFID Technology Scrutinised. RVS Group. Universität Bielefeld; verfügbar unter http://www.rvs.uni-bielefeld.de/publicatons/Reports/SPC2005_Privacy_Enhancing_Technology_Concepts_for_RFID_Technology_Scrutinised.pdf

Hickman, L. J.; Davis, L. M.; Wells, E.; Eisman, M. (2010): Tracking Inmates and Locating Staff with Active Radio-Frequency Identification (RFID). Early Lessons Learned in One U.S. Correctional Facility. Rand Corporation

Hildebrandt, M.; Gutwirth, S. (Hg.): Profiling the European Citizen: Cross-Disciplinary Prospectives. Berlin/ Heidelberg

Hilty, L. M.; Behrendt, S.; Binswanger, M.; Bruinink, A.; Erdmann, L.; Fröhlich, J.; Köhler, A.; Kuster, N.; Som, C.; Würtenberger, F. (2003): Das Vorsorgeprinzip in der Informationsgesellschaft. Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. TA 46/2003. Bern

van't Hof, C.; J. Cornelissen, J. (2006): RFID and Identity Management in Everyday Life. Case Studies on the Frontline of Developments towards Ambient Intelligence. Deliverable No. 2 of the project RFID and Identity Management. commissioned by STOA and carried out by ETAG

van't Hof, C. (2007): RFID and Identity Management in Everyday Life: Striking the balance between convenience, choice and control. European Technology Assessment Group Report. IPOL/STOA/2006-22. Luxemburg

Holtz, L.-E. (2010): Datenschutzkonformes Social Networking: Clique und Scramble!. In: Datenschutz und Datensicherheit 7/2010, S. 439-443

Hyppönen, K.; Hassinen, M.; Trichina, E. (2008): Combining Biometric Authentication with Privacy-Enhancing Technologies. In: Lipp, P.; Sadeghi, A. R.; Koch K. M. (2008): Trusted Computing – Challenges and Applications. Lecture Notes in Computer Science Vol. 4968, Berlin/ Heidelberg, S. 155-165

ICPP (Independent Centre for Privacy Protection), SNG (Studio Notarile Genghini) (2003): Identity Management Systems (IMS): Identification and Comparison Study; verfügbar unter: https://www.daten schutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf

IEMR (IE Market Research Corp.) (2010): Global GPS Navigation and Location Based Services Forecast 2010-2014. 3Q.2010

Ismail, S. (2010): An Evaluation of Students' Identity-Sharing Behaviour in Social Network Communities as Preparation for Knowledge Sharing In: International Journal for the Advancement of Science & Arts 1(1) (2010), S. 14-24

Jovanovic, L. (2010): Handy verrät den Standort. In: RP online vom 24.08.2010; verfügbar unter http://nachrichten.rp-online.de/wirtschaft/handy-verraet-den-standort-1.97705

Juniper (Juniper Research) (2010): Mobile Location Based Services. Applications, Forecasts & Opportunities 2010-2014. Report

Karla, J. (2010): Digitales Vergessen im Web 2.0. In: Wirtschaftsinformatik 52 (2) (2010), S. 105-108

Klüver, L.; Peissl, W.; Tennøe, T.; Bütschi, D. (2006): ICT and Privacy in Europe: Experiences from technology assessment of ICT and Privacy in seven different European countries. Final Report; verfügbar unter http://epub.oeaw.ac.at/ita/ita-projektberichte/e2-2a44.pdf

Koch, M.; Richter, A.; Schlosser, A. (2007): Produkte zum IT-gestützten Social Networking in Unternehmen. In: Wirtschaftsinformatik 49 (6) (2007), S. 448-455

Kölmel, B.; Hubschneider, M. (2003): Nutzererwartungen an Location Based Services. Ergebnisse einer empirischen Analyse; verfügbar unter: http://www.e-lba.com/YellowMap%20AG_Nutzererwartungen%20an%20 Location%20Based%20Services.pdf; abgerufen am 21.06.2010

KPMG (2009): Mobile Payments in Asia Pacific. verfügbar unter: http://www.kpmg.com/AU/en/IssuesAnd Insights/ArticlesPublications/Documents/Mobile-payments-in-Asia-Pacific.pdf; abgerufen 5.10.2009

Kuhlen, R. (2004): Informationsethik. Ethik in elektronischen Räumen. UTB. Konstanz

Lindner, R. (2010): Datenschutz, Umstrittene Privatsphäre à la Facebook. In: FAZ Net Artikel vom 25.05.2010; verfügbar unter: http://www.faz.net/s/RubD16E1F55D21144C4AE3F9DDF52B6E1D9/Doc~ EB6FFF6A871B841B6A8CA40CCDDD1CDB2~ATpl~Ecommon~Scontent.html

van Lieshout, M.; Grossi, L.; Spinelli, G.; Helmus, S.; Kool, L.; Pennings, L.; Stap, R.; Veugen, T.; van der Waaij, B.; Borean, C. (2007): RFID Technologies: Emerging Issues, Challenges and Policy Options; verfügbar unter: ftp://ftp.jrc.es/pub/EURdoc/eur22770en.pdf

van Lieshout, M.; Kool, L. (2008): Little sisters are watching you: A privacy assessment of RFID. In: Fischer Hübner, S.; Duquenoy, P.; Zuccato, A.; Martucci, L. (Hg.): The Future of Identity in the Information Society. Proceedings of the Third IFIP International Summer School 04.-10.08.2007. Karlstad University. Sweden, Berlin/ Heidelberg, S. 129-141

Lischka, K.; Reißmann, O.; Kremp, M. (2011) Your iPhone is watching you, In: Spiegel Online, Artikel veröffentlicht am 20.04.2011, verfübar unter http://www.spiegel.de/netzwelt/web/0,1518,7583 20,00.html

Madlmayr, G.; Ecker, J.; Langer, J.; Scharinger, J. (2008): Near Field Communication: State of Standardization. In: Michahelles, F. (Hg.): First International Conference on the Internet of Things (IOT 2008) – Adjunct Proceedings. Zürich/ St. Gallen, S. 10-15

Mainusch, J.; Burtchen, C. (2010): Kontrolle über eigene Daten in sozialen Netzwerken. In: Datenschutz und Datensicherheit 34(7) (2010), S. 448-452

de Maizière, Th. (2010). Grundlagen für eine gemeinsame Netzpolitik der Zukunft. Rede im Rahmen der Abschlussveranstaltung zur Netzpolitik am 22.06.2010 im Technikmuseum Berlin; verfügbar unter http://www.bmi.bund.de/cln_183/SharedDocs/Reden/DE/2010/06/bm_netzpolitik.html?nn=1200738; abgerufen am 01.08.2010

Mattern, F. (2005): Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen. Berlin/ Heidelberg, S. 1-20

Mayer-Schönberger, V. (2007): Useful void – the art of forgetting in the age of ubiquitous computing. Working Paper. John F. Kennedy School of Government. Harvard University

Mayer-Schönberger, V. (2008): Nützliches Vergessen. In: Reiter, M.; Wittmann-Tiwald, M. (Hg.): Goodbye Privacy – Grundrechte in der digitalen Welt. Wien, S. 9-16

Meusers, R. (2010): Street View? Harmlos gegen Webcams und Luftbilder!. In: Spiegel online vom 23.08.2010; verfügbar unter http://www.spiegel.de/netzwelt/web/a-713226.html

Nitzsche, P. (2010): Achtung, Aufnahme! Filderstadt im Visier von Google Street-View. In: Stuttgarter Wochenblatt vom 26.08.2010

Oertel, B.; Wölk, B. M.; Hilty, L. M.; Köhler, A.; Kelter, H.; Ullmann, M.; Wittmann, S. (2004): Risiken und Chancen des Einsatzes von RFID-Systemen, Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in einer interdisziplinären Kooperation vom IZT – Institut für Zukunftsstudien und Technologiebewertung und der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA). Bonn; verfügbar unter https://www.bsi. bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/RFID/RIKCHA_pdf.pdf?__blob=publicationFile; abgerufen am 18.04.2011

Omni (2010): Omnicard Newsletter vom Oktober 2010; verfügbar unter http://www.omnicard.de/index.php?m =17; abgerufen am 01.10.2010

van Oranje-Nassau, C.; Schindler, R.; Botterman, M. (2009): Policy options for Radio Frequency Identification (RFID) application in healthcare – A prospective view. Final Report (D5). Rand Corporation; verfügbar unter http://ec.europa.eu/information_society/activities/health/docs/studies/rfid/rfid-healthcare-d5v5.pdf

Orwat, C.; Rashid, A.; Wölk, M.; Holtmann, C.; Scheermesser, M.; Kosow, H. (2008): Pervasive Computing in der medizinischen Versorgung. In: Technikfolgenabschätzung – Theorie und Praxis 17(1) (2008), S. 5-12

Pfitzmann, A.; Pfitzmann, B.; Waidner, M. (1988): Datenschutz garantierende offene Kommunikationsnetze. In: Informatik-Spektrum 11/3 (1988), S. 118-142

Punie, Y.; Delaitre, S.; Maghiros, I.; Wright, D. (2006): Dark Scenarios on ambient intelligence: Highlightning risks and vulnerabilities. SWAMI deliverable D2 (Januar 2006); verfügbar unter http://is.jrc.es/pages/TFS/ documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf

Raguse, M.; Meints, M.; Langfeldt, O.; Peissl, W. (2008): Criteria for privacy enhancing security technologies. Bericht des PRISE-Projekt; verfügbar unter http://www.prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_ for_privacy_enhancing_security_technologies.pdf

Rannenberg, K.; Royer, D.; Deuker, A. (2009): Vorwort. In: Rannenberg, K.; Royer, D.; Deuker, A. (Hg.) (2009): The Future of Identity in the Information Society, Challenges and Opportunities. Berlin/ Heidelberg, S. 1-11

Rannenberg, K.; Kahl, C.; Böttcher, K. (2010): Communities, Mobilität und Datenschutz – Innovative Konzepte zum Schutz der Privatsphäre im Projekt PICOS. Forschung Frankfurt 1/2010, S. 42-45

Ray, B. (2008): Mobiles help UK mall strack shoppers' every move. In: The Register vom 20.05.2008; verfügbar unter http://www.theregister.co.uk/2008/05/20/tracking_phones/; abgerufen am 21.06.2010

Redi (2010): EU will Recht auf Vergessen im Netz. SWR3 Info –Nachrichten vom 04.11.2010; verfügbar unter http://www.swr3.de/info/nachrichten/EU-will-Recht-auf-Vergessen-im-Netz/id=47428/did=824146/18f5ud9/index.html; abgerufen am 04.11.2010

Reynolds, F. (2008): Whither Bluetooth?. In: IEEE Pervasive Computing 7(3) (2008), S. 6-8

Richter, A.; Koch, M. (2008): Funktionen von Social-Networking-Diensten. In: Bichler, M. et al. (Hg.) (2008): Gito, S. 1239-1250; verfügbar unter: http://ibis.in.tum.de/mkwi08/18_Kooperationssysteme/04_Richter.pdf; abgerufen am 21.06.2010

Rudlstorfer, D. (2010): Die Preisgabe sensibler Daten im Internet. Möglichkeiten einer Überwachung und ihrer Gefahren. Masterarbeit an der Universität Wien; verfügbar unter https://othes.univie.ac.at/9436/1/2010-04-10_0204396.pdf; abgerufen am 21.06.2010

Roßnagel, A.; Müller, J. (2004): Ubiquitous Computing – Neue Herausforderungen für den Datenschutz. In: Computer und Recht 20(8) (2004), S. 625-632

Sain (2009): Studie der österreichischen Informations- und Koordinierungsstelle Saferinternet.at zu „Web 2.0 als Rahmen für Selbstdarstellung und Vernetzung Jugendlicher", Analyse jugendnaher Plattformen und ausgewählter Selbstdarstellungen von 14- bis 20-jährigen. 1. Teil der Studie „Das Internet als Rezeptions- und Präsentationsplattform für Jugendliche" 2009; verfügbar unter http://www.jff.de/dateien/Bericht_Web_2.0_Selbstdarstellungen_JFF_2009.pdf; abgerufen am 21.06.2010

Sain (2010): Studien der österreichischen Informations- und Koordinierungsstelle Saferinternet.at zu „Chancen und Gefahren von Online Communities". Saferinternet.at ist die österreichische Informations- und Koordinierungsstelle im Safer Internet Netzwerk der EU; verfügbar unter http://www.saferinternet.at/fileadmin/files/Online_Communities_Studie/Ergebnisse_Safer_Internet_Quantitativ_Ultimativ.pdf oder http://www.saferinternet.at/fileadmin/files/Online_Communities_Studie/Bericht_Safer_Internet_qualitativ_Online_Version.pdf

Schmitt, P.; Thiesse, F.; Fleisch, E. (2007): Adoption and Diffusion of RFID Technology in the Automotive Industry. E-DIGIT Workshop. European Conference on Information Systems. St. Gallen

Schubert, M. (2010): Datenschutz: Google Street View speichert WLAN-Netze. In: Netzwelt.de vom 22.04.2010, verfügbar unter http://www.netzwelt.de/news/82527-datenschutz-google-street-view-speichert-wlan-netze.html

Sieker, B.; Ladkin, P. B.; Henning, J. E. (2005): Privacy Checklist for Privacy Enhancing Technology Concepts for RFID Technology Revisited. RVS Group. University Bielefeld; verfügbar unter: http://www.rvs.uni-bielefeld.de/publications/#resreports, abgerufen am 22.07.2010

Smith, D. S.; Cain, M. W.; Mann, J.; Lundy, J.; Bradley, A.; Dulaney, K.; Rozwell, C.; Basso, M. (2009): Predicts 2010: Social Software Is an Enterprise Reality. Gartner Inc.

SpOn (2010): Geodatengesetz. Sammler, über die noch keiner spricht. In: Spiegel Online vom 20.9.2010, verfügbar unter http://www.spiegel.de/netzwelt/netzpolitik/0,1518,718410,00.html

Sterbik-Lamina, J.; Peissl, W.; Čas, J. (2009): Privatsphäre 2.0 – Beeinträchtigung der Privatsphäre in Österreich. TA-Studie der Österreichischen Akademie der Wissenschaften (ÖAW) und des Instituts für Technikfolgenabschätzung (ITA). Wien

Steimel, B.; Paulke, S.; Klemann, J. (2008): Praxisleitfaden Mobile Marketing: Status Quo, Erfolgsfaktoren, Strategien & Trends. Studie herausgegeben von der Zeitschrift „Absatzwirtschaft“. Strateco GmbH & Co. KG. Bad Homburg v. d. Höhe

Stern, M.; Böhm, K.; Buchmann, E. (2010): Processing Continuous Joint Queries in Sensor Networks: a Filtering Approach. In: Proceedings of the 2010 international Conference on Management of Data in Indianapolis, Indiana (USA) vom 06.-10.06.2010. SIGMOD '10. ACM. New York, S. 267-278

Stöcker, C. (2010): Datenschutz bei Facebook, Wie die Privatsphäre erodiert. In: Spiegel Online vom 14.05.2010; verfügbar unter http://www.spiegel.de/netzwelt/netzpolitik/0,1518,694388,00.html; abgerufen am 14.05.2010

Stolfo, S. J.; Tsudik, G. (2010): Privacy-Preserving Sharing of Sensitive Information. In: IEEE Security and Privacy 07/08 (2010), S. 16-17

von Streit, A. (2011): Das Datenschutz-Dilemma der vernetzten Welt: In: Focus-Online, Artikel veröffentlicht am 2704.201, verfügbar unter http://www.focus.de/digital/internet/sony-hackerangriff-das-datenschutz-dilemma-der-vernetzten-welt_aid_621866.html

Symantec (2009): Symantec Internet Security Threat Report. Mountain View 2010; verfügbar unter http://www.symantec.com/business/theme.jsp?themeid=threatreport

Toprak, M; Kutter, S. (2008): Verborgene Fühler. In: Handelsblatt, Artikel vom 10.02.2008; verfügbar unter http://www.handelsblatt.com/technologie/forschung/verborgene-fuehler;1387903

Vanjoki, A. (2010): Nokia's executive vice president for markets, has announced that all new Smartphone introduced by the company from 2011 will come with NFC. In: NFC-Newsticker vom 17. Juni 2010; verfügbar unter http://www.cnm.uni-hannover.de; abgerufen am 21.06.2010

VDI (VDI/VDE Innovation + Technik GmbH) (2007): RFID – Potenziale für Deutschland, Stand und Perspektiven von Anwendungen auf Basis der Radiofrequenz - Identifikation auf den nationalen und internationalen Märkten, Studie für das Bundesministerium für Wirtschaft und Technologie; verfügbar unter http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/rfid-potenziale-fuer-deutschland,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf; abgerufen am 18.04.2011

Weber, A. (2001): High Number of Electronic Cash Transactions in Hong Kong Octopus System. In: ePSO-Newsletter 5 (2001)

Weber, A. (2007): The convergence of mobile data phones, consumer electronics, and wallets. Lessons from Japan. In: Telematics and Informatics 24 (3) (2007), S. 180-191

Weichert, T. (2009): Stellungnahme zur elektronischen Gesundheitskarte anlässlich der öffentlichen Anhörung des Gesundheitsausschusses am 25. Mai 2009; verfügbar unter https://www.daten schutzzentrum.de/ medizin/gesundheitskarte/20090525-weichert-stellungnahme-egk.htm; abgerufen am 21.06.2010

Weiser, M. (1991): The Computer for the 21st Century. In: Scientific American 265(3) (1991), S. 94-104

Weiß, S. (2008): The Need for a Paradigm Shift in Addressing Privacy Risks in Social Networking Applications. In: IFIP International Federation for Information Processing Vol. 262: The Future of Identity in the Information Society. Boston, S. 161-171

Weiß, S. (2010a): Datenschutz Compliance in Sozialen Netzwerk Anwendungen. Voraussetzungen für die technische Umsetzbarkeit. In: Datenschutz und Datensicherheit 34 (7) (2010), S. 444-447

Weiß, S. (2010b): An Information Architecture Framework for Enhancing Privacy in Social Network Applications. INTERNET – Praxis und Zukunftsanwendungen des Internets (Bd.7). Hamburg

Wiedmann, K.-P.; Reeh, M.-O.; Schumacher, H. (2010): Employment and Acceptance of Near Field Communication in Mobile Marketing. In: Pousttchi, K.; Wiedemann, D. G. (Hg.) (2010): Handbook of Research on Mobile Marketing Management. Hershey, S. 190-212

Williamson, D. A. (2010): Worldwide Social Network Ad Spending: A Rising Tide. Report von eMarketer 08/2010

ZDF (2010): Bericht des ZDF Auslandjournals vom 21.07.2010 zu „Verbrechen 2.0“

Zou, C. C. (2006): Physically Changeable Bit for Preserving Privacy. In: Low-End RFID Tags. RFID White Paper Library. RFID Journal; verfügbar unter: http://www.cs.ucf.edu/~czou/research/PCB.pdf

Autorenverzeichnis

Reisch, Sven; Institut für Technikfolgenabschätzung und Systemanalyse, Karlsruher Institut für Technologie (KIT), Campus Nord, Postfach 36 40, 76021 Karlsruhe; Tel.: +49 (0) 721 / 608 - 2 25 01; Fax: +49 (0) 721 / 608 - 2 48 06; E-Mail: sven_reisch@web.de

Weber, Arnd. Dr.; Institut für Technikfolgenabschätzung und Systemanalyse, Karlsruher Institut für Technologie (KIT), Postfach 36 40, 76021 Karlsruhe; Tel.: +49 (0) 721 / 608 - 23737; Fax: +49 (0) 721 / 608 - 24806; E-Mail: arnd.weber@kit.edu; Internet: http://www.kit.edu

Weinberger, Nora. Dipl.-Ing.; Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), Karlsruher Institut für Technologie (KIT), Postfach 36 40, 76021 Karlsruhe; Tel.: +49 (0) 7 21 / 6 08 - 2 3972; Fax: +49 (0) 7 21 / 6 08 - 2 78 90; E-Mail: nora.weinberger@kit.edu; Internet: http://www.kit.edu

Kontaktdaten

Dipl.-Ing. Nora Weinberger
Tel.: +49 (0) 7 21 / 6 08 - 2 39 72
Fax: +49 (0) 7 21 / 6 08 - 2 48 06
E-Mail: nora.weinberger@kit.edu

ITAS – Institutsprofil und Forschungsprogramm

Das Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) erarbeitet und vermittelt Wissen über die Folgen menschlichen Handelns und ihre Bewertung in Bezug auf die Entwicklung und den Einsatz von neuen Technologien. Das ITAS erforscht wissenschaftliche und technische Entwicklungen in Bezug auf systemische Zusammenhänge und Technikfolgen. Umweltbezogene, ökonomische, soziale sowie politisch-institutionelle Fragestellungen stehen dabei im Mittelpunkt. Wesentliche Ziele sind die Orientierung der Forschungs- und Technikpolitik, die Einflussnahme auf die Gestaltung sozio-technischer Systeme im Hinblick etwa auf Kriterien nachhaltiger Entwicklung sowie die Durchführung diskursiver Verfahren zu offenen oder kontroversen technologiepolitischen Fragen. Die Ergebnisse der Forschung und Beratung sind öffentlich.

Für weitere Informationen: http://www.itas.kit.edu

Anschrift

Institut für Technikfolgenabschätzung
und Systemanalyse (ITAS)
Karlsruher Institut für Technologie (KIT)
Postfach 36 40, 76021 Karlsruhe
Leitung: Prof. Dr. Armin Grunwald
Sekretariat: Bettina Schmidt-Leis
Tel.: + 49 (0) 7 21 / 6 08 - 2 25 01
Fax: + 49 (0) 7 21 / 6 08 - 2 48 06