Bundesministerium
für Bildung
und Forschung

TAUCIS

Technikfolgenabschätzung
Ubiquitäres Computing und Informationelle Selbstbestimmung

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Institut für Wirtschaftsinformatik
Humboldt-Universität zu Berlin

TAUCIS

Technikfolgenabschätzung
Ubiquitäres Computing und Informationelle Selbstbestimmung

Studie im Auftrag des Bundesministeriums für Bildung und Forschung

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98, 24103 Kiel, Tel.: 0431 / 988 - 1200, Fax: 0431 / 988 - 1223

mail@datenschutzzentrum.de, http://www.datenschutzzentrum.de/

Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin (HU)

Spandauer Straße 1, 10178 Berlin, Tel.: 030 / 2093 - 5742, Fax: 030 / 2093 - 5741

iwi@wiwi.hu-berlin.de, http://iwi.wiwi.hu-berlin.de/

http://www.taucis.de/ taucis@datenschutzzentrum.de

Projektleitung ULD:
Dr. Johann Bizer

Projektleitung HU:
Dr. Sarah Spiekermann
Prof. Oliver Günther, Ph.D.

Autoren-Team:

Bizer, Johann (ULD)
Dingel, Kai (HU)
Fabian, Benjamin (HU)
Günther, Oliver (HU)
Hansen, Markus (ULD)
Klafft, Michael (HU)
Möller, Jan (ULD)
Spiekermann, Sarah (HU)

Stand: Juli 2006

Das Autoren-Team dankt

Guido Beier, Oliver Berthold, Petra Bulwahn, Matthias Fischmann, Seda Gürses, Jasmin John, Marit Hansen, Kai Janneck, Seçkin Kara, Oliver Kawell, Christian Köster, Martin Meints, Matthias Rothensee und Brigitte Zimmermann für inhaltliche und organisatorische Unterstützung bei der Ausarbeitung der Studie;

Johann Cas, Alexander Dix, Hansjürgen Garstka, Lorenz Hilty, Marc Langheinrich, Frank Pallas, Barbara van Schewick sowie dem Bundesministerium für Bildung und Forschung und dem Projektträger für kritische Anmerkungen und Kommentare zu unseren Überlegungen.

Einleitung

Diese Studie „Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung“ (TAUCIS) ist im Auftrag des Bundesministeriums für Bildung und Forschung (BMBF) als ein Kooperationsprojekt zwischen dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und dem Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin (HU) entstanden. Die Studie wurde vom BMBF im Rahmen der Innovations- und Technikanalyse gefördert. Untersuchungszeitraum war Oktober 2004 bis März 2006.

Gegenstand der Studie ist die zunehmende Allgegenwart der Informationstechnologie (IT), hier ungeachtet sprachästhetischer Aspekte und dem allgemeinen Sprachgebrauch folgend als „Ubiquitäres Computing“ bezeichnet, und dessen Auswirkungen auf die informationelle Selbstbestimmung. Ziel der ersten vier Kapitel ist, ein grundlegendes Verständnis des Konzepts UC zu vermitteln. Zu diesem Zweck beschreiben wir Stand und Entwicklungsperspektiven der technischen Grundlagen des UC (Kap. 1), identifizieren seine zentralen Anwendungsfelder (Kap. 2), analysieren und systematisieren die für die weitere Entwicklung zentralen Bestimmungsfaktoren (Kap. 3) und entwerfen Szenarien, um die zukünftige Wirklichkeit des UC verständlich zu machen (Kap. 4).

In den folgenden Kapiteln setzen wir uns mit den Folgen des UC für die informationelle Selbstbestimmung und den präventiven Gestaltungsmöglichkeiten auseinander. Wir untersuchen vor dem Hintergrund eigener empirischer Untersuchungen die Einstellung der Verbraucherinnen und Verbraucher zu UC (Kap. 5), diskutieren die datenschutzrechtlichen Risiken des Ubiquitous Computing und die Möglichkeiten, ihnen durch rechtliche Maßnahmen zu begegnen (Kap. 6), und untersuchen die sich aus der Technik des UC ergebenden Sicherheitsrisiken und ihre Auswirkungen (Kap. 7). Die Studie schließt mit einer zusammenfassenden Bewertung der Auswirkungen des UC (Kap. 8) sowie unseren Empfehlungen, mit welchen Maßnahmen die zukünftige Entwicklung des UC zu flankieren ist (Kap. 9), um einen adäquaten Datenschutz zu garantieren.

Die Studie wird von den beiden Kooperationspartnern gemeinsam vertreten und verantwortet. Natürlich können Studien eines solchen Umfanges nur arbeitsteilig entstehen. Um dem individuellen Sachverstand und dem spezifischen Engagement der Mitarbeiterinnen und Mitarbeiter Rechnung zu tragen, ist es uns ein Anliegen, ungeachtet der Gesamtverantwortung der beiden Institutionen und ihrer Projektleitung die federführenden Autoren zu Beginn der einzelnen Kapitel namentlich zu nennen.

Kiel/Berlin, den 1. Juni 2006

Johann Bizer Sarah Spiekermann Oliver Günther

Inhaltsverzeichnis

1 Technische Grundlagen

Benjamin Fabian, Markus Hansen

1.1 Was ist „Ubiquitäres Computing“?

Der Begriff des „Ubiquitous Computing“ geht auf Mark Weiser[1] zurück, der in seinem Aufsatz „The Computer for the 21st Century“ seine Vision vorstellte, in der der (Personal-) Computer als Gerät verschwindet und durch „intelligente Gegenstände“ ersetzt wird, die die Menschen bei ihren Tätigkeiten unauffällig unterstützen.[2]

Ubiquitous Computing (allgegenwärtige Datenverarbeitung)[3] bezeichnet die Allgegenwärtigkeit von – in der Regel sehr kleinen – Sensoren, Prozessoren und Aktuatoren, die miteinander kommunizieren und Aktionen auslösen und steuern. Alltagsgegenstände bekommen so die zusätzliche Eigenschaft, sich entsprechend wahrgenommener Umgebungsvariablen zu ‚verhalten’.

Neben Ubiquitous Computing werden auch Begriffe wie „Mobile Computing“ (mobile Datenverarbeitung), „Pervasive Computing“ (durchdringende Datenverarbeitung) und „Ambient Intelligence“ (Intelligenz der Umgebung) verwendet, deren Beziehung zueinander im Folgenden beschrieben wird.

Wenn man den Versuch unternimmt, die Begriffe schärfer zu trennen, so erweisen sich die folgenden Überlegungen als hilfreich. Ausgehend von der „traditionellen“ Datenverarbeitung mit Servern, PCs, Terminals und traditionellen Ein- und Ausgabegeräten als Interface führt eine Erhöhung der Mobilität zum „Mobile Computing“ – eine verstärkte Einbettung miniaturisierter Computer in andere Gegenstände hingegen zum „Pervasive Computing“. Werden beide Aspekte zusammen genommen, so ergibt sich eine allgegenwärtige Datenverarbeitung, das Ubiquitous Computing.

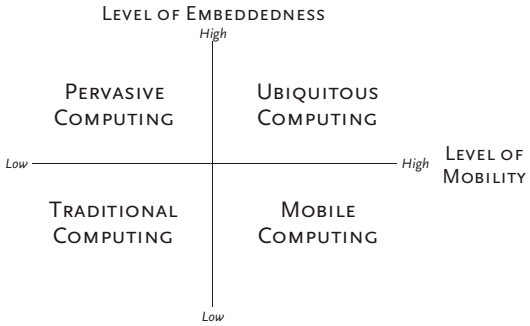


Abbildung 1: Dimensionen des Ubiquitous Computing, aus: Lyytinen / Yoo, 2002.

Pervasive Computing bezeichnet wörtlich die Durchdringung von Alltagsgegenständen mit

[1] Weiser, Mark: http://www.ubiq.com/hypertext/weiser/UbiHome.html (30.03.2006).

[2] Weiser, The Computer for the 21st Century, Scientific American, 265, 3, 1991, S. 66-75; Weiser, Mark, CACM 36(7), Juli 1993. S. 75-84.

[3] Wegweisend zur UC-Forschung: Abowd / Mynatt, ACM Transactions on Computer-Human Interaction, Vol. 7, No. 1, März 2000, S. 29–58.

den genannten Sensoren, Prozessoren oder Aktuatoren.

Ambient Intelligence (Intelligenz der Umgebung) ist ein von der Information Society Technologies Advisory Group der EU[4] geprägter Begriff, der im Wesentlichen Ubiquitous Computing beschreibt, dabei aber zugleich davon ausgeht, dass die bei der Einführung auftretenden Problemfelder (soziale Akzeptanz, detaillierte Verhaltensprofile, Abrechnung von Dienstleistungen etc.) gelöst sind.

Ubiquitous Computing, Pervasive Computing und Ambient Intelligence werden trotz der (zumindest in Detailfragen) vorhandenen Unterschiede häufig synonym verwendet. In der vorliegenden Studie benutzen wir in Anlehnung an Weiser als übergeordnete Bezeichnung den Begriff "Ubiquitäres Computing" (bzw. das englische "Ubiquitous Computing"), abgekürzt „UC“.

In diesem Kapitel werden die technischen Grundlagen von UC behandelt, soweit sie sich bereits heute absehen lassen. Zunächst geben wir einen Überblick über die technischen Eigenschaften, die UC zukommen sollen, und geben eine abstrakte Beschreibung eines adaptiven UC-Systems, wie es für viele Anwendungsszenarien relevant wird.

Dann folgen Abschnitte zu Hardware, Software und Kommunikation, die aufgrund ihrer Bedeutung für Informationssicherheit und informationelle Selbstbestimmung im UC ausführlicher dargestellt werden. Im Anschluss folgt ein Abschnitt zu Mensch-Computer Interaktion, bevor in einer Zusammenfassung der Datenfluss im UC dargestellt wird.

1.2 Technische Eigenschaften von UC-Systemen

Analysiert man UC-Szenarien[5] in Hinsicht auf grundlegende technische Funktionen, so lässt sich aus den Beschreibungen ableiten, dass UC-Systemen folgende Aufgaben zugedacht sind:

- Stetig und überall verfügbare Computerunterstützung („ubiquitär“).
- Stark vereinfachte Schnittstellen zwischen Mensch und Computer, die die Aufmerksamkeit und Interaktion der Nutzer minimal einfordern (Calm Computing[6]).
- Automatische Steuerung und Anpassung der Umgebung an Nutzerpräferenzen oder situative Kontexte.
- Automatische Ausführung und Abwicklung wiederkehrender standardisierter Abläufe ohne Einforderung einer Nutzerinteraktion.

Um dies – zunächst abstrakt – technisch umzusetzen, werden folgende Komponenten[7] be-

[4] ISTAG, 2003.

[5] Vergl. z.B. die Szenarien in Kapitel 4. Siehe auch das EU-Projekt SWAMI, Safeguards in a World of Ambient Intelligence: http://swami.jrc.es/pages/ (17.03.2006).

[6] Weiser / Brown, The Coming Age of Calm Technology, 1996: http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm (06.03.2006).

[7] Derartige Komponenten können sowohl Hard- als auch Software oder Virtualisierungen davon sein.

nötigt:[8]

- Eine verteilte Infrastruktur für Sensoren und Schnittstellen (Interfaces).
- Eine verteilte Infrastruktur für den Transport von Daten.
- Rechenleistung von einem oder mehreren (verteilten) Computern, die Daten verarbeiten und Entscheidungen treffen. Der Entscheidungsalgorithmus sollte adaptiv sein, d.h. sich an unterschiedliche Bedingungen und Kontexte anpassen können (Entwicklung in Richtung künstliche Intelligenz bzw. „Soft Computing“).
- Zugriff auf einen oder mehrere (verteilte) Datenspeicher.
- Anbindung an externe Datenquellen und Dienste.
- Komponenten zur Umsetzung von Entscheidungen bzw. zur Ausführung einer Dienstleistung (Service) oder anderen Aktionen (Aktuatoren[9]), ggf. auch in einer verteilten Infrastruktur.

Das folgende Diagramm stellt die Interaktion eines Nutzers mit einem generischen UC-System auf Grundlage der vorangegangenen Beschreibungen dar. Dabei stehen die Pfeile jeweils für den Transport von Daten zwischen den unterschiedlichen Komponenten des Systems.[10]

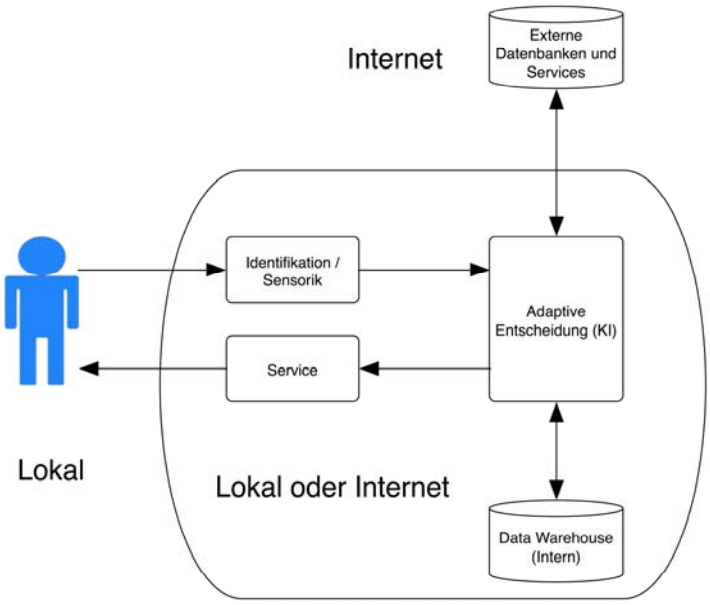


Abbildung 2: Adaptives UC-System

[8] Diese Anforderungen sowie das folgende Diagramm basieren auf Arbeitsergebnissen eines Workshops des Projekts „Future of Identity in the Information Society“ (FIDIS), vergl. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.6.workshop_on_ami_profiling_and_rfid.pdf (30.04.2006).

[9] Aktuatoren oder Aktoren sind Geräte oder Materialien, die aus der Ferne steuerbare Aktionen oder Handlungen ausführen können.

[10] Für eine Betrachtung dieses generischen Systems aus Datensicherheitssicht vergl. Kapitel 7.

Der Mensch (oder ein Objekt) wird vom UC-System mittels Sensoren erfasst und (optional) identifiziert. Diese Informationen fließen zusammen mit Daten aus internen und externen Datenquellen in eine adaptive Entscheidungsfindung ein, die den zu erbringenden Dienst (Service) steuert und Aktionen auslöst.

Derartige Systeme werden in unterschiedlichen Abstufungen modularisiert sein. D.h. neben der Existenz von „All-in-one"-Lösungen ist insbesondere auch denkbar, dass sich aus einzelnen, verteilten und heterogenen Komponenten jeweils diejenigen für die Dauer einer Leistungserbringung miteinander zu einem System vernetzen, die aufgrund besonderer Eigenschaften gerade benötigt werden und über entsprechende freie Kapazitäten verfügen. So können auch bei Wiederholung gleicher Abläufe unterschiedliche Komponenten beteiligt sein. Diese können sich dynamisch zu einem UC-System zusammenfinden, ohne dass für den Nutzer offensichtlich ist, welche Komponenten genau zur Zeit genutzt werden.

Aufgrund dieser prinzipiellen Offenheit von Systemen ist es von grundsätzlicher Bedeutung, Sicherheitsmaßnahmen multilateral anzulegen, d.h. die einzelnen Komponenten (und auf einer höheren Ebene auch einzelne Teilsysteme) müssen auch über jeweils Sicherheitsmechanismen voreinander verfügen. Nur so kann gewährleistet werden, dass im Fall der Kompromittierung einer Komponente der Rest des Systems nicht automatisch ebenfalls kompromittiert wird.

Prototypisch für UC-Systeme lassen sich z.B. RFID-Systeme betrachten. Dabei dienen Identifikatoren auf RFID-Tags dazu, Objekte zu erkennen, für deren Erkennung per se z.B. (noch) keine geeigneten Sensoren verfügbar sind, bzw. um unterschiedliche Objekte mit einheitlichen Sensoren (hier RFID-Reader) erfassen zu können. Aus diesem Grund wird in den folgenden Kapiteln intensiver auf RFID-basierte Ansätze eingegangen. Als weitere Beispiele für zentrale UC-Technologien lassen sich auch allgemeine Sensor- und Ad-hoc-Netze sowie Location-based Services als prototypisch für UC-Systeme betrachten, d.h. Dienste, die den Aufenthaltsort des Nutzers miteinbeziehen.[11]

Eine wichtige Erkenntnis ist, dass UC-Systeme die Eigenschaften und Anforderungen ihrer Komponenten und der diesen zugrunde liegenden Basistechnologien erben. Dies ist insbesondere in Fragen von Datenschutz und Datensicherheit relevant, zumal die Kombination der Eigenschaften und Anforderungen der Einzelkomponenten über die „Summe" hinaus völlig neue Dimensionen der Datenverarbeitung eröffnen kann.

Die Verbindung und Integration unterschiedlicher Komponenten sowie deren Entwicklungsrichtung und Geschwindigkeit bilden wichtige Faktoren, die die Gesamtheit des Ubiquitous Computing beeinflussen, weshalb in den folgenden Abschnitten dieses Kapitels relevante Basistechnologien vorgestellt werden, die diese Komponenten bilden oder auf oder zwischen ihnen zum Einsatz kommen.

[11] Zur notwendigen Lokalisierung der Nutzer können diese Dienste wiederum z.B. auf Sensornetze, RFID, WLAN, Bluetooth oder GSM zurückgreifen.

1.3 Hardware

1.3.1 Miniaturisierung

Die fortschreitende Miniaturisierung von Computerhardware ermöglicht die Einbettung von Chips in die Gegenstände unserer Umwelt: Computer werden allgegenwärtig. Ein erster Vorläufer dieser Entwicklung ist die RFID-Technologie.[12]

Das berühmte so genannte „Gesetz" von Moore[13] sagt voraus, dass sich die Integrationsdichte von integrierten Schaltkreisen, d.h. die Anzahl von Transistoren pro Flächeneinheit, etwa alle 18 Monate verdoppelt. Ob und wie lange dieser Trend anhält, ist umstritten, ebenso, ob er sich verlangsamen oder beschleunigen wird. Die Genauigkeit der Vorhersage über die letzten Jahrzehnte ist allerdings bemerkenswert.

Zum einen wird Hardware konstanten Umfangs und Preises immer leistungsfähiger, zum anderen können immer kleinere und billigere Chips mit Standardfunktionen wie zum Beispiel Netzwerkfunktionalität ausgestattet werden. Diese Geräte werden als so genannte eingebettete Computersysteme („Embedded Systems") in immer mehr Alltagsgegenstände integriert.

Einen neuen Entwicklungshorizont bildet die Nanotechnologie, die im Größenmaßstab eines Milliardstel Meters arbeitet.[14] Sie wird die Entwicklung immer kleinerer Computer und Maschinen mittel- und langfristig weiter vorantreiben. Mit Atomen als Bausteinen für Nanomaschinen wird möglicherweise eine natürliche Grenze der Miniaturisierung und ein finaler Entwicklungshorizont erreicht werden, allerdings sind absolute Aussagen über Grenzen der Miniaturisierung mit einer gewisser Vorsicht zu genießen.

1.3.2 Energie

Vorangetrieben durch den Drang zu immer leistungsfähigeren mobilen Geräten ist eine starke Entwicklung im Bereich der mobilen Energieversorgung zu beobachten.[15] Neben der Verbesserung von Energiespeichern und der Minimierung des Energieverbrauchs von Komponenten sind die drahtlose Energieübertragung als auch eine mobile Energiegewinnung wichtige Schwerpunkte in Forschung und Entwicklung.

Energiespeicher sind heute in der Regel wiederaufladbar. In der Serienproduktion werden für mobile Geräte derzeit Lithium-Ionen-Akkus eingesetzt.

Brennstoffzellen auf Basis von Wasserstoff, Methanol oder Methan sollen als mobile Energielieferanten eingesetzt werden. Aufgrund der Gewinnung des Brennstoffs aus nachwach-

---

[12] Siehe Kap. 1.5.2.1.1.

[13] Intel über Moore: http://www.intel.com/research/silicon/mooreslaw.htm (31.01.2006).

[14] Zur Nanotechnologie siehe z.B.: http://www.nanotechnology.de/ ; http://www.cfn.uni-karlsruhe.de/ ; http://www.foresight.org/ (31.01.2006); Lauterwasser, Opportunities and Risks of Nanotechnologies, 2005.

[15] Fraunhofer ISC: http://www.isc.fraunhofer.de/german/geschaeftsfelder/gf4/ (30.03.2006).

senden Rohstoffen wird für Brennstoffzellen gemeinhin eine positive Ökobilanz angenommen. Allerdings legen jüngere Untersuchungergebnisse[16] nahe, dass zumindest im Fall von Wasserstoff dies aufgrund der für die Produktion benötigten Energie nicht der Fall ist.[17]

Während einzelne Modelle z.B. bereits auf U-Booten der Bundesmarine im Echtbetrieb eingesetzt werden, sind für den Einsatz in UC-Komponenten hinreichend kleine Modelle noch im Entwicklungsstadium. Aufgrund der Nachfüllproblematik ist davon auszugehen, dass Brennstoffzellen nur in vergleichsweise großen Geräten (PDA oder größer) zum Einsatz kommen werden. Ebenso ist bei eingebetteten Komponenten die Wahl einer nachladebedürftigen Energieversorgung eher ungünstig, da aufgrund der Einbettung der Zugang zum Energiespeicher möglicherweise sehr erschwert ist.

Drahtlose Energieübertragung wird z.B. im Bereich von passiven Transpondern (RFID) eingesetzt.[18] Die Transponder nutzen für den eigenen Betrieb und die Übermittlung eines Antwortsignals die Energie des elektromagnetischen Feldes des Senders. Auch gezielte Energieübertragung mittels Laser befindet sich bereits in Produktiv-Systemen im Einsatz. Ziel ist es, Verluste während der Übertragung zu minimieren und Reichweiten zu maximieren. Forschungsprojekte arbeiten daran, im Weltraum gewonnene Solarenergie auf die Erde zu transferieren.[19] Mit einem die Erde umfassenden Netz an Anlagen zur Energiegewinnung und Relaisstationen wäre auf diese Weise eine flächendeckende Versorgung mit elektrischer Energie möglich.

Im Bereich der mobilen Energiegewinnung sind neben den bereits verbreiteten Systemen auf der Basis von Solarzellen[20] (z.B. Ladegräte für Mobiltelefone oder komplett solarbetriebene Geräte) neue Ansätze in der Entwicklung, die elektrische Energie z.B. aus Lärm, Bewegung oder Temperaturunterschieden gewinnen können.[21] Diese Forschungsergebnisse ermöglichen relativ autarke Systeme, die unabhängig von Leitungsanbindungen eingesetzt werden können.

Energiesparsamkeit, die ausreichende Miniaturisierung von Brennstoffzellen und neue Me-

[16] Heise News, http://www.heise.de/newsticker/meldung/71466 (31.03.2006), verweist diesbezüglich auf eine noch unveröffentlichte Studie im Auftrag des Umweltbundesamtes (UBA).

[17] Grundlegende Studie zu den Auswirkungen von UC auf Gesundheit und Umwelt: Hilty et al., The Precautionary Principle in the Information Society – Effects of Pervasive Computing on Health and Environment, 2005, http://www.empa.ch/sis (17.03.2006).

[18] Finkenzeller, RFID-Handbuch, 2002.

[19] Siehe Innovations-Report, Drahtlose Energie-Übertragung aus dem All, http://www.innovations-report.de/html/berichte/energie_elektrotechnik/bericht-29342.html (30.01.2006).

[20] Zu Forschungen zur Leistungsverbesserung von Photovoltaik-Anlagen siehe http://www.hindu.com/seta/2005/02/03/stories/2005020300431600.htm (30.03.2006).

[21] Militärische Forschung zu sogenannten „Smart Exhaust Systems“: http://www.foster-miller.com/projectexamples/wearhome/smart_exhaust_system.htm (30.01.2006).

thoden zum „Ernten“ von Energie aus der Umgebung[22] bilden neue Entwicklungsschritte auf dem Weg zur Verwirklichung von UC.

1.3.3 Intelligente Materialien

In der Materialforschung werden so genannte „Intelligente Materialien“ (Smart Materials)[23] entwickelt. Eine Definition gibt McCloskey: Smart materials are „non-living material systems that achieve adaptive behaviour“.[24] Hierzu gehören Verbundwerkstoffe mit integrierten piezoelektrischen Fasern, elektrisch und magnetisch aktive Polymere und so genannte „Shape Memory Alloys“ (SMA), d.h. Metalllegierungen, die nach einer Verformung einfach durch Erhitzung ihre ursprüngliche Gestalt wieder annehmen. Zum Bereich der intelligenten Materialien kann man auch Mikro-elektromechanische Systeme (MEMS) zählen, d.h. Kombinationen aus mechanischen Elementen, Sensoren, Aktuatoren und elektronischen Schaltungen auf einem Substrat bzw. Chip.

Diese Verbundwerkstoffe können sowohl sensorische Funktionen, wie das Erfassen und Lokalisieren von physischer Beanspruchung (z.B. an einem Flugzeugflügel), als auch aktuatorische bzw. effektorische Funktion übernehmen, d.h. zum Beispiel durch elektrische Ansteuerung eine Bewegung oder Verformung erzeugen.

Organische Polymerchips sollen insbesondere im Bereich der RFID-Tags zu niedrigeren Stückkosten führen. Beispiel für Forschungen zu Polymerchips ist das EU-geförderte Projekt PolyApply[25] sowie Ansätze, Chips durch Drucktechnik herzustellen[26].

1.3.4 Neue Bauformen

Kleinere Bauteile, die weniger Energie verbrauchen und ggf. aus neuen Materialien bestehen, lassen neue Bauformen zu. Auf diese Weise ist es leichter möglich, mobile Systeme zu entwickeln, die sich dynamisch miteinander in Kommunikationsbeziehung setzen.

Als bekanntestes Beispiel bezeichnet Wearable Computing die Integration von Systemen in Kleidung. Während in der einfachsten Form ein eingewebtes RFID-Tag (vergl. Kap. 1.5.2.1.1) das Objekt elektronisch identifizierbar macht, leisten komplexere Systeme erheblich mehr: Die Kleidung wird Eingabemedium, Daten verarbeitendes System, Ausga-

[22] Zum allgemeinen Problem eines „Batteriewechsels“ im UC und weiteren Lösungsansätzen siehe Satyanarayanan, Energy Harvesting & Conservation, IEEE Pervasive Computing, Vol. 4, No. 1, January-March 2005.

[23] Forschung z.B. bei Fraunhofer, http://www.smart-materials.fhg.de/ (30.01.2006), siehe auch http://www.cs.ualberta.ca/~database/MEMS/sma_mems/smrt.html (30.01.2006).

[24] McCloskey, Paul: From RFID to Smart Dust, 2004.

[25] Projekt PolyApply (The Application of Polymer Electronics to Ambient Intelligence): http://www.polyapply.org/ (30.01.2006).

[26] Implementierung z.B. bei http://www.polyic.com/ (30.01.2006).

bemedium und Kommunikationsschnittstelle. Dazu werden Sensoren, Microcontroller[27], Displays etc. in die Kleidung integriert. Neben einer optimalen Anpassung der Kleidung an aktuelle Umgebungsparameter und das Verhalten des Trägers lassen sich auf diese Weise auch zusätzliche Funktionen wie die eines Mobiltelefons oder eines PDAs in die Kleidung integrieren.

Ein in erster Linie für militärische Anwendungen konzipiertes Beispiel ist Smart Dust.[28] Dabei handelt es sich um winzige (1 mm^3 und kleiner) hochintegrierte Systeme, die in großen Mengen eingesetzt werden, sich miteinander vernetzen, ihre Umgebung über enthaltene Sensoren überwachen und die dabei anfallenden Daten an eine Basisstation übermitteln. Für diese äußerst unauffällige Überwachung gibt es zahlreiche zivile und militärische Einsatzszenarien.

1.3.5 Sensorik

Ubiquitous Computing basiert unter anderem auf einer möglichst vollständigen Wahrnehmung der Umgebung durch IT-Systeme. Sensoren können Daten über ihre Umwelt erfassen und an verarbeitende Systeme weiterleiten, die die Messwerte mit Referenzwerten abgleichen und entsprechende Reaktionen einleiten können.

Die Entwicklung im Bereich der Sensorik[29] hat in den letzten Jahren beträchtliche Fortschritte verzeichnet. Neben optischen und akustischen[30] Sensoren, mit denen die menschlichen Wahrnehmungsfähigkeiten z.T. bei weitem übertroffen werden können, sind auch olfaktorische Sensoren[31] verfügbar. Sensoren zur Messung von Temperatur, Luftfeuchtigkeit, Druck, elektromagnetischen Feldern, Abstand zwischen Objekten, Position, Geschwindigkeit etc. werden ebenfalls immer feiner auflösend und dabei kostengünstiger und in kleinerer Form produzierbar.

1.3.6 Universalität mobiler Geräte

Während mobile Geräte wie Telefone oder PDAs in den ersten Generationen zunächst auf vorgegebene Abläufe beschränkt waren, arbeiten aktuelle Geräte mit eigenen Betriebssystemen, auf denen prinzipiell beliebige Anwendungen (innerhalb der Einschränkungen der Hardware) installiert werden können. Beschränkungen ergeben sich aus einer eingeschränkten Leistungsfähigkeit der jeweiligen Systeme (Hardware und Betriebssystem), ihrer mangelnde Dokumentation sowie aus künstlichen Barrieren zur Wahrung von Geschäftsmodellen

[27] Kranz, 2004.

[28] Marculescu / Marculescu / et al., 2003. Thoms; 2003; Pister / Kahn / Boser, Smart Dust, http://robotics.eecs.berkeley.edu/~pister/SmartDust/ (30.03.2003).

[29] Zhang, Angewandte Sensorik, 2003.

[30] Stäger / Lukowicz / Tröster, 2004.

[31] Boeker, Technisch-sensorische Geruchsmessung, 2004.

(z.B. Digital Rights Management), die verhindern sollen, dass beliebige Anwendungen installiert werden können.

Die gesteigerte Universalität der mobilen Geräte hat zur Folge, dass über sie auch neue Dienste (z.B. Location-Based Services, Mobile Commerce) angeboten werden können. Zu beobachten ist ferner ein Verschmelzen unterschiedlicher mobiler Geräte zu einem. So haben bspw. aktuelle Mobiltelefone (Smart Phones) in der Regel auch PDA-Funktionen (bzw. lassen sich moderne PDAs auch als Telefon nutzen). Sie können sich nicht nur bei Telefon-Netzen anmelden, sondern auch drahtlose Netzverbindungen per WLAN und Bluetooth nutzen. Geräte mit mehreren verschiedenen Netzzugängen werden auch als Hybridgeräte bezeichnet.

1.4 Software

1.4.1 Verteilte Systeme

Unter verteilten Systemen[32] versteht man allgemein Softwarearchitekturen, die die gemeinsame Nutzung von Rechenkapazitäten auf verschiedenen Rechnern eines Netzwerks erlauben. Dieser Vorgang kann transparent erfolgen, so dass ein ablaufendes Programm nicht unbedingt Kenntnis davon haben muss, wo genau Teile seines Codes ausgeführt werden.

Ein klassisches Beispiel für verteilte Systeme ist CORBA[33], ein Standard der Object Management Group (OMG), der unter anderem Programmierschnittstellen (API), Kommunikationsprotokolle und eine „Interface Description Language“ (IDL) zur Definition von Objektschnittstellen bereitstellt. Diese allgemeinen Definitionen erlauben eine Implementierung in verschiedenen Programmiersprachen.

Klassische verteilte Systeme benutzen meist eine Client-Server-Architektur, in der diese Rollen relativ festgelegt sind. In Peer-to-Peer-Systemen (P2P) hingegen ist diese Rollenverteilung flexibel und kann sich dynamisch ändern.[34]

Im Bereich des Ubiquitous Computing werden verteilte Systeme durch die Vielzahl interagierender mobiler und eingebetteter Rechner eine sehr große Bedeutung erlangen, da erst durch diese Softwarearchitekturen höher gelagerte Anwendungen und Dienstleistungen möglich werden. Dazu ist insbesondere die Entwicklung von entsprechender Middleware als Abstraktions- und Vermittlungsebene zwischen den einzelnen Komponenten wichtig.[35]

---

[32] Greenberg, Network Application Frameworks, 1999; Birman, Reliable Distributed Systems, 2005; zu den Sicherheitsproblemen bei der praktischen Imlementierung siehe Anderson, Security Engineering, 2001.

[33] „Common Object Request Broker Architecture“. Siehe OMG Homepage: OMG, http://www.omg.org/ (30.02.2006).

[34] Steinmetz / Wehrle (Hrsg.), Peer-to-Peer Systems and Applications, 2005.

[35] Tandler, Software Infrastructure for Ubiquitous Computing Environments, 2001; Schoch, Thomas: Middleware für Ubiquitous-Computing-Anwendungen, in: Fleisch / Mattern (Hrsg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, 2005, S. 119-140.

1.4.1.1 Dienstbasierte Architekturen (SOA)

Der Begriff der dienstbasierten Architektur (Service-Oriented Architecture, SOA) beschreibt eine verteilte Softwarearchitektur, bei der Dienste an verschiedenen Stellen in einem internen Netzwerk oder im Internet auf heterogenen Systemen und Entwicklungsplattformen verfügbar sind, aber dennoch eine hohe Interoperabilität aufweisen. Meistens kommen dabei webbasierte Dienste (Web Services) zum Einsatz.[36]

In dienstbasierten Architekturen wird eine neue Form der Nutzung von Software möglich, indem Kundensysteme auf die von Anwendungsdienstleistern (Application Service Provider, ASP) angebotenen Dienste bei Bedarf aus der Ferne zugreifen können (On-Demand Architectures).

> *"Ein ASP stellt einer Vielzahl von Kunden garantierte Dienstleistungen zur Nutzung einer Anwendungssoftware im Rahmen eines Mietvertrages zur Verfügung. Die Anwendungssoftware wird zentral in einem Datenzentrum verwaltet und beherbergt. Kunden können über Netzwerke auf die gemietete Anwendungssoftware und Dienstleistungen zugreifen. Die Zahlung der Nutzungsgebühr garantiert regelmäßig die Bereitstellung der Software, die Pflege und Wartung der Server im Datenzentrum und Leistungen des Kundenservice. Hierbei kann der ASP alle primären und sekundären Aktivitäten der ASP-Wertschöpfung selbst oder mit Hilfe eines Partnernetzwerkes bereitstellen."*[37]

Verschiedene Anbieter stellen Werkzeuge zur Umsetzung von dienstbasierten Architekturen zur Verfügung, wie zum Beispiel die Frameworks von Sun (J2EE) und Microsoft (.NET), SAP Netweaver oder IBM Web Sphere.

Dienstbasierte Architekturen werden in erweiterter Form besonders auch im Ubiquitous Computing enorme Bedeutung erlangen, da einerseits eine neue Dimension der allgemeinen Vernetzung erreicht wird, andererseits ein hoher Grad an Automatisierung, Flexibilität und Qualität in der Nutzung ubiquitärer Softwaresysteme nötig wird.

1.4.1.2 Webbasierte Dienste (Web Services)

Webbasierte Dienste (Web Services)[38] nutzen offene und standardisierte Protokolle zum Datenaustausch zwischen Anwendungen. Als Format für den Datenaustausch dient XML (eXtensible Markup Language). Die Dienste selbst werden mit WSDL (Web Service Description Language) genau beschrieben und spezifiziert. SOAP (Simple Object Access Protocol) regelt die Kommunikation zwischen den beteiligten Webdiensten mittels Nachrichten, die eingebettet in HTTP, FTP oder SMTP als Übertragungsprotokollen, das Netz durchqueren.

Um zum Beispiel Dienste für bestimmte Zwecke lokalisieren zu können, steht mit UDDI[39] (Universal Description, Discovery and Integration) ein Protokoll bereit, das eine zentrale Re-

[36] Tamm / Günther, Webbasierte Dienste, 2005.

[37] Ibid., S. 21.

[38] Chappell / Jewell, Java Web Services, 2003.

[39] OASIS Homepage zu UDDI: http://www.uddi.org/ (30.03.2006).

gistrierung von webbasierten Diensten in offen zugänglichen Verzeichnissen und ihre automatische Klassifikation anhand verschiedener Taxonomien ermöglicht.

Vorteile von Web Services sind die rein textbasierten Protokoll- und Datenformate und die einfache Kommunikation über Standardprotokolle, was ihren Einsatz durch hohe Interoperabilität erleichtert. Nachteile im Vergleich etwa zu CORBA sind bisher fehlende Transaktionen (im Sinne der Datenbanktechnik) und geringere Performanz. Dass sich verteilte Systeme via HTTP durch klassische Firewalls „tunneln" lassen, kann je nach Sichtweise als Vorteil durch Flexibilität oder als Sicherheitsproblem betrachtet werden.

1.4.1.3 Grid Computing

Eine weitere spezielle Form verteilter Systeme bildet das Grid Computing[40], bei dem die im Netzwerk angebotenen Dienste und Ressourcen im wesentlichen aus angebotener Rechenleistung und Speicherkapazität bestehen, die transparent von entfernten Systemen aus flexibel genutzt werden kann. In gewissem Sinne werden temporäre globale Cluster aus verschiedensten Computern möglich.

Im Ubiquitous Computing ist es denkbar, dass relativ rechenschwache, kleine Geräte sich bei Bedarf die Rechenleistung stationärer Geräte ihrer Umgebung leihen können, um bestimmte zeitlich begrenzte Aufgaben zu erfüllen.

1.4.1.4 Peer-to-Peer-Architekturen

Peer-to-Peer-Architekturen (P2P)[41] ermöglichen eine wesentlich flexiblere Handhabung der Funktionen Client und Server, als es in klassischen verteilten Systemen möglich ist. Beide Rollen können jeweils gleichzeitig von allen beteiligten Knoten in einem Netzwerk ausgeübt werden. Peer-to-Peer-Netzwerke sind also wesentlich dezentraler und bestehen üblicherweise aus gleichberechtigten Partnern.

Insbesondere sind P2P-Ansätze bei der Bildung von spontanen, so genannten „Ad-hoc"-Netzen – zum Beispiel in bestimmten Sensornetzen – und den dort entstehenden Dienstarchitekturen wichtig. Als eine quasi natürliche Organisationsform bietet sich P2P für viele Bereiche des Ubiquitous Computing aufgrund der Vielzahl der beteiligten Geräte und der Spontaneität ihrer Vernetzung an.[42]

1.4.2 Kontextwahrnehmung

Ein wichtiger Aspekt im Ubiquitous Computing ist die Wahrnehmung des Kontextes durch

---

[40] Grid Computing Info Centre: http://www.gridcomputing.com/ (30.03.2006); Wikipedia, s.v. Grid Computing, http://en.wikipedia.org/wiki/Grid_computing (30.03.2006); Für Implementierungs-Framework und Analysen http://www.globus.org/ (30.03.2006).

[41] Steinmetz / Wehrle (Hrsg.), Peer-to-Peer Systems and Applications, 2005.

[42] Beispielsweise Protokolle im Projekt JXTA: http://www.jxta.org/ (30.03.2006).

Geräte („Context Awareness“).[43] Ohne für jede einzelne Aktion explizit konfiguriert werden zu müssen, sollen sie sich flexibel auf die jeweiligen Erfordernisse einstellen können. Ein einfaches Beispiel ist eine Raumbeleuchtung oder Tapetenfarbe, die sich stets nach den Vorlieben eines Menschen richtet, der den Raum betritt.

Man kann drei wichtige Komponenten unterscheiden: Wahrnehmung von Identität, Aktivität und Zustand eines Nutzers, Wahrnehmung der physischen Umgebung sowie die Selbstwahrnehmung von Geräten, also Erkennen des eigenen Status. Im erweiterten Sinne zählt hierzu auch, dass Computer den Kontext von Daten, insbesondere von Dokumenten verstehen.[44] Dies führt unter anderem zur Entwicklung eines „semantischen Webs“, das von Softwareagenten interpretiert werden kann.[45]

1.4.2.1 Personenerkennung und Verhaltensanalyse

Damit sich Umgebungssysteme auf einen Nutzer einstellen können, müssen sie ihn und seinen aktuellen „Zustand“ erkennen und daraus die gerade erwünschte Umgebungseinstellung ableiten. Dies leistet Software, die die von Sensoren gelieferten Daten auswertet.

Die Identifizierung von Personen über biometrische Merkmale befindet sich seit ein paar Jahren in der Markteinführung, jedoch handelt es sich dabei noch um Systeme, die eine aktive Mitarbeit des Nutzers voraussetzen. So ist es für einen Scan von Fingerabdruck oder Iris erforderlich, Finger oder Auge gezielt zu positionieren. Weniger aufwendig sind Erkennungssysteme, die die menschliche Stimme als zu erkennendes Merkmal nutzen.[46] In der Entwicklung befinden sich Systeme, die Personen auch ohne das Abfordern konkreter Aktionen erkennen können. Dies ist einerseits für die Nutzer bequem, andererseits aber auch sehr problematisch, da generell eine Identifikation von Personen auch ohne deren Einverständnis ermöglicht wird.

Die Wahrnehmung der Aktivität und des Verhaltens der Nutzer wird ebenfalls über Software realisiert. Dabei gibt es sowohl Software, die „ihren Nutzer“ zunächst mittels Sammlung von Profildaten kennenlernen muss, um die volle Leistungsfähigkeit zu erreichen (dies trifft in der Regel auch auf Schrift- und Spracherkennungssysteme zu), aber auch Programme, die unabhängig von Profildaten Auswertungen vornehmen, zum Beispiel um während eines Telefonates durch Auswertung der akustischen Daten einzuschätzen, ob der Gesprächspartner lügt.

[43] Schmidt, Ubiquitous Computing – Computing in Context, 2002; Projekt TEA zur „Context Awareness“: http://www.teco.edu/tea/tea_vis.html (30.03.2006).

[44] Überblick über dazu notwendige Verfahren aus dem Bereich „Soft Computing“: Aliev / Fazlohalli / Aliev: Soft Computing and its Applications in Business and Economics, 2004.

[45] Berners-Lee, Weaving the Web, 2000. Siehe auch Kap. 1.4.2.2.

[46] Löwer, 2004.

1.4.2.2 Semantisches Web

Eine Weiterentwicklung des herkömmlichen WWW (World Wide Web) stellt das sogenannte „semantische Web“[47] dar, das die Interpretation der im Web gespeicherten Information durch Computer ermöglichen soll.

> *"The Web was designed as an information space, with the goal that it should be useful not only for human-human communication, but also that machines would be able to participate and help. One of the major obstacles to this has been the fact ... that the structure of the data is not evident to a robot browsing the web."*[48]

Dies beinhaltet aber nicht automatisch, Computer natürliche Sprachen in beliebiger Komplexität verstehen zu lassen – stattdessen beschränkt man sich auf eine präzise definierte Semantik. Technisch ermöglicht werden soll diese Vision durch den Einsatz von RDF (Resource Description Framework)[49], das eine offene Plattform zur Formulierung von Metadaten – gemeint sind Daten, die Webressourcen beschreiben – darstellt. Zur Formulierung nutzt RDF den Standard XML, ist aber darauf nicht beschränkt.

1.4.3 Software-Agenten

Software-Agenten[50] sind spezielle Computerprogramme, die unabhängig agieren (autonom), auf Änderungen in offenen und dynamischen Umgebungen reagieren (reaktiv), eigenständig Aktionen auslösen (proaktiv) und mit anderen Agenten kommunizieren können. Einsatzmöglichkeiten sind die Erledigung von Routineaufgaben und Informationsrecherche. Voraussetzung für den Einsatz von Agentensystemen ist einerseits eine Kontextwahrnehmung, um bspw. den Benutzerwillen zu erkennen und gefundene Informationen mithilfe des semantischen Webs in gewissem Sinne zu verstehen, andererseits eine gewisse "Intelligenz", um aus diesen Informationen Entscheidungen ableiten zu können.

Im Ubiquitous Computing wird voraussichtlich ein großer Teil der Interaktion der Nutzer mit den intelligenten Umgebungen an Agenten delegiert werden, die anhand gespeicherter Profile – wie z.B. Nutzerpräferenzen – und eigenen Schlussfolgerungen die menschliche Aufmerksamkeit entlasten sollen. Diese aufgrund wachsender Komplexität notwendige Delegation von Aufgaben kann mit einem Verlust an direkter Kontrolle über das technische Geschehen einhergehen.

1.5 Kommunikation

Einen konzeptionellen Überblick über die Kommunikationstechnologien im Ubiquitous Computing gibt das folgende Schema in Form eines Stundenglases. Im unteren Teil sieht man

---

[47] Berners-Lee, Weaving the Web, 2000.

[48] Berners-Lee, Semantic Web Roadmap, 1998.

[49] RDF Spezifikation, http://www.w3.org/TR/PR-rdf-syntax/ (30.03.2006).

[50] Siehe z.B. das AgentLink Project, http://www.agentlink.org/roadmap/ (30.03.2006); Wikipedia, s.v. Software-Agent, http://de.wikipedia.org/wiki/Software-Agent (30.03.2006).

die Vielfalt der verschiedenen Zugangstechnologien, die die Bitübertragungs- und Sicherungsschicht nach dem OSI-Referenzmodell bilden können.

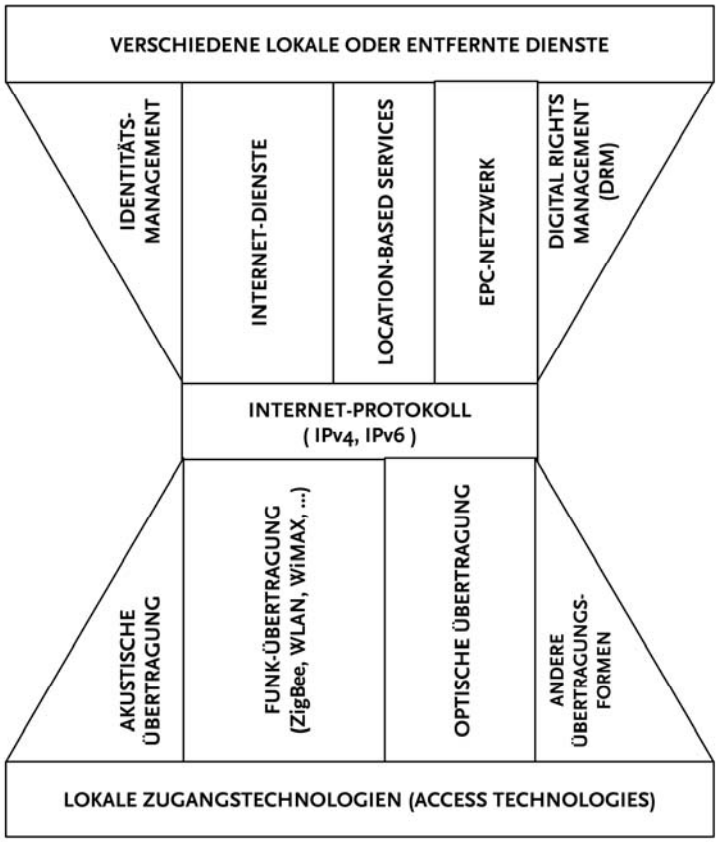


Abbildung 3: Konvergenz: Zugriff auf Dienste via IP

Das Internetprotokoll in seiner jetzigen und zukünftigen Version (IPv6) wird bei vielen Geräten die Vermittlungsschicht bilden und den Zugang zu entfernteren Netzwerkknoten sowie dem Internet ermöglichen. Über dieser einheitlichen Vermittlungsschicht liegt wiederum eine Vielfalt an möglichen Anwendungen und Diensten, die sowohl im lokalen Umfeld als auch aus der Ferne angeboten und genutzt werden können.

Um diese Kommunikationsschichten richtig einordnen zu können, geben wir zunächst einen Überblick über zwei technische Referenzmodelle der Kommunikation.

1.5.1 OSI-Referenzmodell und TCP/IP

Zur Beschreibung von Kommunikationstechnologien hat die International Standards Organization (ISO) ein Schichtenmodell entworfen, das so genannte OSI-Referenzmodell (Open Systems Interconnection).[51] Dieses Schichtenmodell liefert eine logische Strukturierung der Nachrichtenübermittlung zwischen Kommunikationspartnern.

[51] ISO Standard ISO/IEC 7498-1:1994.

Die Schichten L1 und L2 beschreiben die direkte physikalische Kommunikation benachbarter Systeme. Erst die Vermittlungschicht L3 ermöglicht die Adressierung von Nachrichten an entfernte Systeme, hier sind z.B. die IP-Protokolle IPv4 und IPv6 sowie der Vorgang des Routings (Wegfindung) angesiedelt.

Die Transportschicht L4 kann unter anderem die Zuverlässigkeit der Nachrichtenübertragung und Flusskontrolle gewährleisten. Die höheren Schichten beinhalten Verwaltung von logischen Verbindungen, einheitliche Datenrepräsentation und Kommunikation mithilfe höherer Anwendungsprotokolle.

In der praktischen Anwendung hat sich anstelle des OSI- das TCP/IP-Referenzmodell durchgesetzt.[52] Dieses einfachere Modell enthält nur vier anstelle von sieben Schichten.

	OSI-Modell		**TCP/IP**	
L7	Anwendungsschicht (Application Layer)		Anwendungsschicht (Application Layer)	T4
L6	Darstellungsschicht (Presentation Layer)			
L5	Kommunikationsschicht (Session Layer)			
L4	Transportschicht (Transport Layer)		Transportschicht (Transport Layer)	T3
L3	Vermittlungsschicht (Network Layer)		Internetschicht (Internet Layer)	T2
L2	Sicherungsschicht (Data Link Layer)		Netzwerkschicht (Network Layer)	T1
L1	Bitübertragungsschicht (Physical Layer)			

Abbildung 4: Die OSI- und TCP/IP-Referenzmodelle

Mithilfe dieser beiden Referenzmodelle lassen sich die diversen einzelnen Kommunikationstechnologien entsprechend ihrer Funktionen in die Schichten einordnen.

Im Anschluss beschreiben wir wichtige Kommunikationstechnologien für Ubiquitous Computing, wobei wir uns in den Kommunikations-Modellen aufwärts bewegen.

[52] Fundamental zu TCP/IP: Stevens, TCP/IP Illustrated, Volume 1 – The Protocols, 1994.

1.5.2 Bitübertragungs- und Sicherungsschichten (Netzwerkschicht)

Auch im Ubiquitous Computing wird der Hauptteil der Backend-Kommunikation über leitungsgebundene Kommunikationsnetze übertragen werden (metallische Leiter, Glasfaser), woraus immer intensiveren Anforderungen hinsichtlich der verfügbaren Bandbreite folgen.

Von spezifischem Interesse im Sinne des Ubiquitous Computing sind allerdings die nichtleitungsgebundenen Übertragungsverfahren, auf die im Folgenden eingegangen wird. Die physikalische Reichweite einer Technologie kann ein wichtiges Kriterium sein, ob sie sich für den Einsatz in einem BAN (Body Area Network, auch: Human Area Networks), PAN (Personal Area Network), LAN (Local Area Network) oder gar MAN (Metropolitan Area Network) oder WAN (Wide Area Network) eignet. Diese Reichweite ist eine Eigenschaft der jeweiligen Zugangstechnologie auf der Bitübertragungsschicht.

1.5.2.1 Funkübertragung

Funktechnologien bilden den Schwerpunkt unter den drahtlosen Kommunikationstechnologien. Wir behandeln wichtige Einzeltechnologien, indem wir sie nach ihrer ungefähren physischen Reichweite einordnen.

1.5.2.1.1 Transponder / RFID

Radio Frequency Identification (RFID, deutsch: Identifizierung per Funk) dient dem kontaktlosen Speichern und Auslesen von Daten.[53] Die Daten werden auf so genannten RFID-Tags (kleine Etiketten) gespeichert, die nahezu überall befestigt werden können. Die Kommunikation mit RFID-Tags kann je nach Modell über Distanzen von wenigen Zentimetern bis ca. 30 Metern erfolgen.

Man unterscheidet zwischen aktiven Tags mit eigener Energieversorgung und passiven Tags, die ihre Energie aus dem elektrischen Feld eines Lesegeräts (Reader) beziehen. Passive Tags verwenden aufgrund ihrer schwachen Leistungsfähigkeit kein TCP/IP, was aber mittelfristig für aktive Tags durchaus möglich ist.

Eine weitere Einteilung der Tags richtet sich nach dem verwendeten Frequenzbereich und den damit verbundenen Reichweiten.

Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete / normale Reichweite	Übertragungsart
6,75 MHz	-	44 Meter	1 Meter	Induktive Kopplung
13,56 MHZ	Früher: Supply-Chain-Management	3,5 Meter	1 Meter	Induktive Kopplung

[53] Grundlegend Finkenzeller, 2002. Ausführliche Behandlung in Garfinkel / Rosenberg (Hrsg.): RFID Applications, Security, and Privacy, 2005; Fleisch / Mattern (Hrsg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, 2005. Siehe auch das Projekt InterVal der HU Berlin: http://interval.hu-berlin.de/rfid/ (30.03.2006).

	(Trend geht zu UHF)			
UHF (865-928 MHz)	Supply-Chain-Management	unbegrenzt	7 Meter	Backscatter

Tabelle 1: Reichweiten passiver Tags (Spiekermann / Ziekow, 2005)

Frequenz	**Hauptanwendung**	**Theoretische Reichweite**	**Berichtete / normale Reichweite**	**Übertragungsart**
UHF (865-928 MHz)	Mautsystem (z.B. Österreich)	unbegrenzt	15-30 Meter	Backscatter

Tabelle 2: Reichweiten aktiver Tags

Schließlich unterscheidet man Tags auch nach der Speichertechnologie, die zum Einsatz kommt. Es gibt Read-Only-Transponder, die nach einmaligem Beschreiben beim Hersteller nur noch gelesen werden können, und Read-Write-Transponder, die mehrfach beschreibbar und damit flexibler, aber teurer sind.

RFID-Tags können jedes Objekt mit einer eindeutigen Kennung versehen, anhand derer sich Informationen zu diesem Gegenstand mit einer Datenbank abgleichen lassen. Einen weltweiten Nummern-Standard stellt der so genannte „Electronic Product Code“ (EPC)[54] dar, der die eindeutige Identifizierung und Unterscheidung von Objekten erlaubt.

Dies bietet im Logistikbereich Vorteile, ist aber nicht ohne Folgen für die Privatsphäre: Da für das Lesen der Kennung kein Sichtkontakt erforderlich ist, ist es für eine Person auch nicht bemerkbar, wenn sie auf RFID-Tags gescannt wird, von denen sie vielleicht gar nicht weiß, dass sie diese mit sich führt.[55]

Im Ubiquitous Computing ist es für ein Hintergrundsystem so möglich, Objekte eindeutig zu identifizieren und damit die vorhandene Umgebung zu erkennen. Sofern eine Identifizierung von Personen nicht über z.B. biometrische Systeme erfolgen kann, ist dies über von der Person mitgeführte Transponder möglich. Die Einbettung von RFID-Systemen in Reisepässe und Personalausweise wird diskutiert. Sie sollen eine eindeutige Erkennung und Überwachung von Personen theoretisch ermöglichen. In einigen Diskotheken und auch Krankenhäusern werden Menschen kleine Transponder injiziert, um sie zu identifizieren und zu lokalisieren.

[54] EPCglobal RFID Standards: http://www.epcglobalinc.com/standards_technology/specifications.html (30.03.2006); dort besonders EPC Radio-Frequency Identity Protocols – Class-1 Generation-2 UHF RFID, 2004.

[55] Bundesamt für Sicherheit in der Informationstechnik (BSI): Risiken und Chancen des Einsatzes von RFID-Systemen, 2004, http://www.bsi.bund.de (06.03.2006); Hansen / Wiese, DuD 28, 02/2004, S. 109, 2004; Berthold / Günther / Spiekermann, Wirtschaftsinformatik 6 (47), 2005, S. 422 – 430.

1.5.2.1.2 ZigBee

Bei ZigBee[56] handelt es sich um einen neuen Wireless Personal Area Network (WPAN) Standard[57], der besonders für niedrige Datenraten und geringen Energieverbrauch konzipiert ist, und auch als spezielle, semi-aktive RFID-Variante für Sensorik und Kontrollfunktionen z.B. in der Hausautomatisierung betrachtet werden kann.

1.5.2.1.3 Bluetooth

Bluetooth[58] ist ein Standard für drahtlose Übertragung im Nahbereich. Bluetooth kommt insbesondere zum Einsatz, um Geräte wie Drucker, Handy, Scanner kabellos miteinander zu verbinden, ist aber prinzipiell auch für eine IP-basierte Rechner-Vernetzung geeignet, darum erfolgt hier die Einordnung unter den übrigen Accesstechnologien.

Bluetoothgeräte sind in so genannten Piconets aus zwei bis acht Geräten organisiert, wobei eines die Rolle eines „Masters" einnimmt. Piconets können sich unter Umständen überlappen, dann spricht man von einem „Scatternet". Der genutzte Frequenzbereich liegt im ISM-Band bei 2,4 GHz bei recht niedriger Ausgangsleistung. Je nach verwendeter Version liegen die offiziellen Reichweiten bei 10 bis 100 Metern, bei Tests mit Richtantennen sind aber schon wesentlich höhere Reichweiten erzielt worden.

Im Gegensatz zu WLAN unterstützt Bluetooth einen regelmäßigen Frequenzwechsel und erschwert damit sowohl ein Stören wie ein Abhören der Verbindung. Allerdings genügt es, ein Datenpaket abzufangen, um an die Hardware-Adresse zu gelangen, die die Frequenzen definiert. Der in Bluetooth implementierte 128-Bit-Algorithmus „Safer+" (abgeleitet von DES) kann theoretisch gebrochen werden, wenn es einem Angreifer gelingt, einen ausreichend langen Datenstrom mitzuschneiden. Bisherige erfolgreiche Angriffe richteten sich eher gegen Fehler in spezifischen Implementationen.[59] Da jedes Bluetooth-Gerät über einen eindeutigen Identifizierungscode verfügt, ist es möglich, Personen z.B. anhand ihres Handys mit Bluetooth-Funktion zu identifizieren und zu verfolgen, ohne dass es von ihnen bemerkt wird.

Seit Mai 2005 kooperiert die Bluetooth Special Interest Group (SIG) mit Entwicklern der Ultra-Wideband-Technik (UWB), um eine drastische Steigerung der Übertragungsgeschwindigkeit zu erzielen.

1.5.2.1.4 WLAN (IEEE 802.11)

WLAN (Wireless Local Area Network, deutsch: drahtloses lokales Netz)[60] ist ein Verfahren zur drahtlosen Datenübertragung. Dies ermöglicht PCs und anderen Geräten eine Vernetzung ohne auf die Verlegung von Kabeln angewiesen zu sein und ist daher insbesondere für

---

[56] ZigBee Alliance, http://www.zigbee.org/ (30.03.2006).

[57] IEEE 802.15 WPAN Task Group, http://ieee802.org/15/pub/TG4.html (30.03.2006).

[58] Bluetooth Spezifikationen, https://www.bluetooth.org/spec/ (30.03.2006); Roth, Mobile Computing, 2002, S. 142-170.

[59] Hurman / Rowe, WBF2004.

[60] Rech, Wireless LANs, 2004; Schiller, Mobile Communications, 2003, S. 201-301.

den Anschluss mobiler Geräte an das Internet und die Bildung von Ad-hoc-Netzen (vergl. 1.5.3.3) interessant.

Die folgende Tabelle gibt einen Überblick über die Standards nach IEEE 802.11.[61]

Standard	Inhalt	Jahr	Bemerkung
IEEE 802.11	2,4 GHz (ISM), max. 2 MBit/s	1997	Der ursprüngliche Standard
IEEE 802.11a	5 GHz, max. 54 MBit/s	1999	
IEEE 802.11b	2,4 GHz, max. 11 MBit/s	1999	
IEEE 802.11e	Quality of Service (QoS)		„Wireless Mutimedia Enhancements“ (WME); Draft
IEEE 802.11f	Inter Access Point Protocol (IAPP)	2003	Informationsaustausch in der festen Infrastruktur
IEEE 802.11g	2,4 GHz, max. 54 MBit/s	2003	
IEEE 802.11h	5 GHz für Europa	2003	Anpassung von IEEE 802.11a
IEEE 802.11i	MAC Security Enhancements	2004	Neue Spezifikationen zur Sicherheit
IEEE 802.11n	Max. 320 MBit/s		In Vorbereitung

Abbildung 3: WLAN-Standards nach IEEE 802.11

Da die Kommunikation über Funk leicht abhörbar ist, sahen die ersten WLAN-Standards ein Sicherheitskonzept WEP (Wired Equivalent Privacy) vor. Seit Herbst 2000 wurden allerdings immer mehr Lücken in WEP der ersten WLAN-Standards bekannt. Bereits im Sommer 2001 waren alle verwendeten Zugangskontrollmechanismen und die Verschlüsselung gebrochen. Frei erhältliche Tools zum Ausnutzen der bekannten Lücken machten dies zu einem allgemeinen Problem.[62]

Inzwischen ist daher mit WPA (Wi-Fi Protected Access) bzw. WPA2 ein neues Sicherheitskonzept eingeführt worden, das bisher als noch nicht gebrochen gilt.[63] WPA kann als Vorstufe des neuen Standards IEEE 802.11i betrachtet werden, der unter anderem Mechanismen wie TKIP (Temporary Key Integrity Protocol), AES (Advanced Encryption Standard) und RADIUS-Authentifizierung vorsieht.

1.5.2.1.5 HiperLAN

HiperLAN (High Performance Radio LAN) bzw. HiperLAN/2 sind Standards des ETSI (Euro-

[61] IEEE 802.11 Standards: http://standards.ieee.org/getieee802/ (30.03.2006).

[62] Vladimirov et al.: WI-FOO, 2004; Sankar, Krishna / et al.: Cisco Wireless LAN Security, Indianapolis, 2005.BSI, Sicherheit im Funk-LAN (WLAN, IEEE 802.11): http://www.bsi.bund.de/literat/doc/wlan/ (30.03.2006).

[63] Krishna et al.: Cisco Wireless LAN Security, 2005; ULD zu WLAN: http://www.datenschutzzentrum.de/material/tb/tb26/kap10.htm#Tz10.1 (30.03.2006).

pean Telecommunications Standards Institute)[64] und stellen eine Alternative zu WLAN nach IEEE 802.11 dar. Beide Versionen von HiperLAN arbeiten im 5 GHz-Frequenzband, HiperLAN/2 mit maximal 54 MBit/s. HiperLAN hat sich am Markt nicht durchgesetzt, allerdings gibt es Firmen, die Produkte für HiperLAN/2 auf den Markt bringen.[65]

1.5.2.1.6 WiMAX

WiMAX[66] ist die Bezeichnung für drahtlose „Wide Area Network"- (WAN) bzw. „Wireless Metropolitan Area Network"-Standards (WMAN, IEEE 802.16, ETSI HiperMAN). Ziel sind neben hoher Reichweite auch hohe Bandbreiten, man spricht auch von „Broadband Wireless Access" (BWA).

1.5.2.1.7 Mobiltelefonie

Mobiltelefonie hat seit der Markteinführung in den 1990er Jahren eine hohe Marktdurchdringung erreicht. In Deutschland / Europa kommt dabei der Kommunikationsstandard GSM (Global System for Mobile Communication)[67] zum Einsatz, der vorherige analoge Systeme ablöste. In Einführung befindet sich der neue Standard UMTS (Universal Mobile Telecommunication System)[68], der dafür ausgelegt ist, breitbandigere Datenverbindungen zu erlauben als mit GSM und seinen Erweiterungen möglich ist. In der Planungsphase sind bereits so genannte Netze der 4. Generation (4G Networks), die ihrerseits UMTS ablösen sollen.

Mobiltelefonie ist in Deutschland nahezu flächendeckend verfügbar. Dazu gibt es ein großes Netz einzelner Funkzellen, die über Richtfunkstrecken und Kabelleitungen miteinander verbunden sind. Die Kommunikationsdienstleistungen werden von unterschiedlichen Anbietern zur Verfügung gestellt. Zum Teil ist dabei ein sog. Roaming möglich, d.h. die Nutzung von Funkzellen eines anderen Anbieters, was in der Regel zusätzliche Kosten für den Nutzer bewirkt. Roaming ermöglicht aber oftmals die Nutzung eines Mobiltelefons mit einem in einem Land abgeschlossenen Vertrag auch in anderen Ländern.

Damit Ubiquitous Computing auch wirklich ubiquitär, d.h. allgegenwärtig wird, muss es auch für UC-Dienstleistungen Anbieter geben, die idealerweise auch ein Roaming unterstützen. Forschungsprojekte im Bereich des Ubiquitous Computing können hier wahrscheinlich viel von den Erfahrungen der Mobilfunkanbieter lernen.

1.5.2.1.8 Satellitengestützte Positionsbestimmung

Für einige Anwendungen des Ubiquitous Computing ist es notwendig, die Position von Personen und Objekten zu bestimmen. Satellitengestützte Systeme wie das amerikanische GPS

---

[64] ETSI HIPERLAN/2 Standard: http://portal.etsi.org/radio/HiperLAN/HiperLAN.asp (30.03.2006); Rech: Wireless LANs, Hannover, 2004, S. 9-11.

[65] Palowireless Resource Center: http://www.palowireless.com/hiperlan2/products.asp (30.03.2006).

[66] WiMAX Forum: http://www.wimaxforum.org/ (30.03.2006); IEEE 802.16 Working Group: http://ieee802.org/16/ (30.03.2006).

[67] GSM Association: http://www.gsmworld.com/index.shtml (30.03.2006); Chaos Computer Club zu GSM: http://www.ccc.de/gsm/ (30.03.2006).

[68] UMTS Report: http://www.umts-report.com/umts.php (30.03.2006).

(Global Positioning System)[69], das europäische System GALILEO[70] und das russische GLONASS (GLObales NAvigations-Satelliten-System)[71] erlauben eine solche weltweite Lokalisierung. Daneben gibt es noch weniger bedeutende asiatische Systeme, die in Planung bzw. auf den asiatischen Raum beschränkt sind.

Dazu werden die von mehreren Satelliten ständig abgegebenen spezifischen Signale von speziellen Empfangsgeräten ausgewertet, die aus den Signallaufzeiten ihre Höhe und Position sowie bei Ausnutzung des Doppler-Effekts ihre Geschwindigkeit errechnen können. Um die Empfangsgeräte nutzen zu können, muss eine freie Sichtlinie von deren Antennen zu den Satelliten bestehen, die von Bodenstationen aus gesteuert werden.

Da das amerikanische GPS auch militärisch genutzt wird, lässt sich das Signal künstlich derart verschlechtern, dass nur spezielle militärische Geräte noch eine genaue Positionsbestimmung durchführen können, während zivile Geräte, die frei verkäuflich sind und daher auch von vermeintlichen Feinden genutzt werden können, gestört werden. Für das europäische Galileo ist eine künstliche Signalverschlechterung derzeit nicht vorgesehen. Allerdings sind Funksignale in der Regel anfällig für so genanntes Jamming, d.h. das Aussenden von Störsignalen.

Die Auswertung der Satellitensignale durch ein Empfangsgerät erlaubt in der Regel eine Positionsbestimmung mit einer Genauigkeit von unter 10 Metern. Werden zusätzlich Signale von anderen Empfängern, deren genaue Position bekannt ist, ausgewertet, lassen sich unter entsprechenden Bedingungen Genauigkeiten im Millimeterbereich erreichen.

1.5.2.1.9 Optische Übertragung

Die optische Übertragung von Daten ist auf eine Sichtverbindung zwischen Sender und Empfänger angewiesen. Schon geringe Störungen wie Nebel, Regen, durchfliegende Vögel etc. können sich negativ auf die Qualität der Übertragung auswirken. Da Licht sich zudem schneller ausbreitet als Radiowellen im Funkspektrum, lassen sich mit geeigneten optischen Übertragungsverfahren höhere Datenübertragungsraten erzielen.

1.5.2.1.10 Barcode

Die einfachste Form optischer Datenübertragung ist das Scannen optischer Markierungen, wie sie durch die unterschiedlichen Formen eines Barcodes bekannt ist. Dabei wird auf Objekten (z.B. Produktverpackung) im einfachsten Fall ein Code aufgedruckt, der es Hintergrundsystemen (z.B. Warenannahme) erlaubt, gespeicherte Datensätze (z.B. Warenbestand, Preisinformation) zuzuordnen. Die Informationen sind dabei in ein Muster aus unterschiedlich reflektierenden Flächen (z.B. schwarze und weiße Striche) eingebettet. Ein Lesegerät bestrahlt die Muster mit Licht und wertet die Reflektion aus.

[69] Wikipedia, s.v. GPS: http://de.wikipedia.org/wiki/Global_Positioning_System (30.03.2006).

[70] GALILEO Projekt: http://europa.eu.int/comm/dgs/energy_transport/galileo/index.htm (30.03.2006).

[71] GLONASS: http://www.glonass-center.ru/frame_e.html (30.03.2006).

Barcodes[72] sind sehr preiswert; insbesondere im Bereich von Konsumgütern werden die Verpackungen in der Regel ohnehin bedruckt, so dass gar keine Mehrkosten entstehen. Aufgrund von Standardisierungen (Universal Product Code, UPC, in den USA bzw. European Article Number Code, EAN, in Europa)[73] ist zudem der reibungslose Austausch von Gütern gewährleistet.

1.5.2.1.11 Infrarot

Bekannt ist in erster Linie die Datenübertragung im infraroten Bereich des Lichtspektrums, wie sie von der Infrared Data Association (IrDA)[74] standardisiert wurde. IrDA galt lange Zeit als der Standard für die Ad-hoc-Kommunikation mobiler Geräte (Notebooks, Mobiltelefone, PDAs etc.). Infrarot-Schnittstellen finden sich immer noch auf diesen, verlieren jedoch insbesondere durch die Verbreitung von funkbasierten Techniken wie Bluetooth, die nicht auf eine Sichtverbindung angewiesen sind, zunehmend an Bedeutung. Im Ubiquitous Computing sind Infrarot-Schnittstellen dennoch von Interesse, um vorhandene Geräte, die sich per Infrarot fernbedienen lassen (z.B. Fernseher, Videorekorder etc.), in die Steuerung durch die Hintergrundsysteme einzubinden.

1.5.2.1.12 Laser

Aufgrund der geringen Streuung des Laser-Lichts eignet sich dieses für eine gerichtete Datenübertragung,[75] mit der hohe Reichweiten erzielt werden können. So plant die NASA unter anderem, Lasersysteme für die Kommunikation mit Mars-Sonden einzusetzen.[76]

Interessant für Ubiquitous Computing sind Lasersysteme, die auf sehr kleinen Objekten untergebracht werden können und wenig Energie benötigen. Forschung an solchen Systemen findet sich vor allem im Bereich von Smart Dust.[77] Neben aktiver wird dort auch mit passiver Laserkommunikation experimentiert. Dabei werden Objekte an bestimmten Stellen mit einem Laser angestrahlt. Das Objekt ist dabei in der Lage, in einem bestimmten Winkel einfallendes Licht moduliert an die Quelle zu reflektieren und so Daten zu übermitteln. Sofern die Quelle selbst bereits moduliertes Licht sendet, ist eine bidirektionale Kommunikation möglich, die jedoch nur an einer Stelle einen hohen Energiebedarf hat. In einer UC-Umgebung könnte so eine Basisstation mehrere Objekte per Laser mit Energie versorgen (vergl. Kap. 1.3.2) und auf gleichem Weg mit ihnen kommunizieren.

Aufgrund der Gerichtetheit von Laser-Licht stellt sich als Hauptproblem heraus, dass die

---

[72] Vault Information Services, Barcode Symbology: http://www.barcodeisland.com/symbolgy.phtml (30.03.2006).

[73] Adams Communications, Vergleich UPC/EAN: http://www.adams1.com/pub/russadam/upccode.html (30.03.2006).

[74] Infrared Data Association (IrDA): http://www.irda.org/ (30.03.2006); http://www.infraredsystems.net/faq.htm (30.03.2006).

[75] Buse, Karsten: Optische Datenübertragung, Universität Bonn, http://pi.physik.uni-bonn.de/hertz/Papers/talks/041213KB.pdf (30.03.2006).

[76] NewScientist, 16.04.2004: http://www.newscientist.com/article.ns?id=dn6409 (30.03.2006).

[77] Thoms, Smart Dust, 2003.

einzelnen Systeme wissen müssen, wo sich der jeweilige Kommunikationspartner gerade befindet, damit die Laser und ggf. die Empfänger entsprechend ausgerichtet werden können.

1.5.2.2 Akustische Übertragung

Schall als Übertragungsweg für Informationen bietet einige Vorteile: Man benötigt keine direkte Sichtlinie wie etwa bei optischer Übertragung; außerdem lässt sich Schall relativ gut in und durch feste Hindernisse wie Wände übertragen.

Eine Einsatzmöglichkeit ist die Nutzung von Ultraschall, so zum Beispiel im „Active Bat"-System der AT&T Laboratories in Cambridge.[78] Hierbei handelte es sich um ein Lokalisierungssystem für Personen oder Objekte in geschlossenen Räumen, das ein älteres, infrarotbasiertes System namens „Active Badge" ablöste. An den Decken der Laborräume befanden sich Ultraschallempfänger, die die kurzen, regelmäßigen Schallimpulse der kleinen mobilen Sender („Bats", Fledermäuse) empfingen. Mithilfe von Trilateration (Positionsbestimmung anhand von Abständen) ließen sich Ort und auch Bewegung der Sender ermitteln.

Eine andere Variante des Einsatzes von Schallwellen sind akustische Modems. Sie dienen neben ihrem klassischen Anwendungsfeld der Kommunikation über Telefonleitungen seit längerem auch zur Datenübertragung in Unterwasserumgebungen, etwa in der Ozeanographie.[79] Akustische Modems lassen sich für digitale Kommunikation über Luftschnittstellen im Ubiquitous Computing nutzen. Insbesondere bei geringen Datenraten und über kurze Entfernungen ist ihr Einsatz denkbar.[80]

Ein Beispiel für die Nutzung von Schall im hörbaren Bereich ist das Projekt „Digital Voices"[81] beim Xerox PARC, wo auch der Bereich der Ästhetik der verwendeten Signale berücksichtigt wird.

1.5.2.3 Andere Übertragungsverfahren

Im Bereich der „Body Area Networks" (BAN, auch „Personal" oder „Human Area") sind Technologien entwickelt worden, die die elektrischen Eigenschaften des menschlichen Körpers zur Signalverbreitung nutzen.[82] So kann zum Beispiel ein Signalweg zwischen zwei Geräten in verschiedenen Händen hergestellt werden, so zum Beispiel auch beim Händedruck zweier Personen.

---

[78] Cambridge University Computer Laboratory / AT&T: The Bat Ultrasonic Location System, http://www.cl.cam.ac.uk/Research/DTG/attarchive/bat/ (30.03.2006); Stajano, Security for Ubiquitous Computing, 2002, S. 37-40.

[79] UCONN FRONT NOPP Projekt (Ozeanographie): http://www.nopp.uconn.edu/ADCP/ (30.03.2006).

[80] Lopes / Aguilar, IEEE Pervasive Computing 2(3), Juli-September, 2003.

[81] Digital Voices Projekt: http://www.ics.uci.edu/~lopes/dv/dv.html (30.03.2006).

[82] IBM Think Research: The Body Electric, http://domino.research.ibm.com/comm/wwwr_thinkresearch.nsf/pages/pan197.html (30.03.2006); IBM PAN Fact Sheet: http://www.almaden.ibm.com/cs/user/pan/pan.html (30.03.2006); NTT RedTacton: http://www.redtacton.com/en/info/index.html (30.03.2006).

1.5.3 Vermittlungsschicht (Internetschicht) und Transportschicht

1.5.3.1 Internetprotokoll und IPv6

Mittelfristig werden sehr viele UC-Systeme über eine Internetanbindung verfügen, sei es als Teil eines umfassenderen Netzes oder auch nur zur Fernsteuerung und Informationsbeschaffung. Damit wird allerdings auch Informationssicherheit im Internet[83] bedeutsam für UC.

Notwendig für eine Internetverbindung sind das Vorhandensein einer IP-Adresse und das Nutzen von Routing.

Im Jahre 1995 hat die Internet Engineering Task Force (IETF) einen Nachfolger für das Internetprotokoll IP bestimmt: IPv6 (IP Version 6).[84] Bisher ist die ältere Version IPv4 dominant geblieben, wobei sich allerdings vor allem in asiatischen Ländern mit knappem IPv4-Adressraum und bei mobilen Geräten ein großflächiger Einsatz von IPv6 andeutet.

Da die Adressen bei IPv6 128 Bit lang sind, erhält man einen wesentlich umfangreicheren Adressvorrat als bei IPv4 mit seinen 32-Bit Adressen. Die dadurch mögliche großzügige Zuteilung von Subnetzen führt unter anderem auch zu einer Vereinfachung der internetweiten Routingtabellen. Ein vereinfachter IP-Header und die Auslagerung von Optionen in so genannte „Extension Headers“ und eine Vermeidung von Fragmentierung entlasten die Router zusätzlich.

In der Form von IPSEC (IP Security) ist ein Teil der Sicherheitsprotokolle von IPv6 für IPv4 rückportiert worden, allerdings ist ihre Implementierung bei IPv6 verbindlich.

Von Beginn an war Mobilität von vernetzten Geräten ein wichtiger Designfaktor bei IPv6, man erwartete schon damals ihren großen Anteil am Internet. Neben der Autokonfiguration, der automatischen Generierung einer IP-Adresse aus einem von Routern bekanntgegebenem „Präfix“, spielt dabei vor allem das Protokoll Mobile IPv6 eine große Rolle, das besonders sehr mobile Geräte mit häufig wechselnden Aufenthaltsorten und Netzanbindungen unterstützt.

Als mittlerer Entwicklungshorizont zeichnet sich bei mobilen Geräten eine Konvergenz auf dem Network Layer zu IPv6 ab, unabhängig von dem physikalischen Access-Verfahren (etwa WLAN, Bluetooth, UMTS). Migrations- und Tunnelverfahren werden die Verbindung zur etablierten IPv4- Infrastruktur ermöglichen und die Integration der ubiquitären Geräte in bestehende Netze erleichtern.

1.5.3.2 Mobile IP

Hohe Mobilität von Geräten in IP Netzwerken führt zu Problemen bei bestehenden TCP-

[83] Eckert, Claudia: IT-Sicherheit, Oldenbourg Verlag, 3. Auflage, 2004; Bless et al., Sichere Netzwerkkommunikation, 2005.

[84] RFC 2460; Hagen, IPv6 Essentials, 2002; Hagino, IPv6 Network Programming, 2005; Loshin, IPv6, 2004.

Verbindungen oder wenn das Gerät selbst Dienste anbietet, die vom Internet aus erreichbar bleiben sollen, auch wenn sich die IP Adresse des Gerätes durch die Bewegung oft ändert. Das DHCP (Dynamic Host Configuration Protocol) als alleinige Maßnahme genügt zu einer Lösung nicht. Will man nicht auf technische Kniffe wie der Registrierung der dynamischen IP-Adresse unter einem festen DNS-Namen (z.B. DynDNS[85]) zurückgreifen, benötigt man ein systematisches Verfahren.

Mobile IP[86] liefert eine Lösung mithilfe folgender Grundidee: Dem mobilen Gerät wird zunächst eine feste Heimadresse („Home Address“) zugeordnet, unter der es als Dienstanbieter im Internet auftreten kann.

Bewegt sich das Gerät und wird Teil eines anderen IP-Subnetzes, so erhält es eine zweite IP-Adresse („Care-of-Address“), die zum neuen Netz passt. Ein so genannter Heimagent („Home Agent“) dient im Heimnetz als Stellvertreter des Gerätes; er nimmt die an die Heimadresse gerichteten Pakete an und sendet sie über ein IP-Tunnelverfahren an die augenblickliche IP-Adresse des mobilen Geräts.

Für IPv6 soll Mobile IPv6 als Standardkomponente fest in jede IP-Implementierung integriert werden, wohingegen Mobile IPv4 nur eine optionale Komponente ist.

1.5.3.3 Routing in Ad-hoc-Netzen

Im Gegensatz zu stationären, meist hierarchisch strukturierten Netzen sind Ad-hoc-Netze spontane und sehr dynamische Gebilde mit häufiger Änderung der Netzwerktopologie.[87] Entscheidend sind Standort und Reichweite der einzelnen meist drahtlosen Stationen, die sich einerseits selbst nicht auf das Vorhandensein von festen Routern verlassen können, andererseits sich auch an der Weiterleitung fremder Pakete beteiligen sollten.

Wie im stationären Fall existieren diverse Routingprotokolle zur Routenfindung zwischen den beteiligten Stationen.[88] Sie müssen sich adaptiv an die hoch dynamische Landschaft eines Ad-hoc-Netzes anpassen können, wo Knoten wesentlich häufiger verschwinden oder neu erscheinen. Hierbei stellen sich auch Fragen nach der Sicherheit und Zuverlässigkeit der Zwischenstationen, womit Aspekte wie Vertrauen und Reputation relevant werden.

1.5.4 Beispiele für Dienste auf höheren Schichten

1.5.4.1 Lokale Dienstvermittlung

Ein Beispiel für eine Architektur der lokalen Dienstvermittlung auf höheren Netzwerkschich-

[85] DynDNS Homepage: http://www.dyndns.com (30.03.2006).

[86] RFC 2002, 2977; Soliman, Mobile IPv6, 2004.

[87] Ilyas, The Handbook of Ad Hoc Wireless Networks, 2003; Roth, Mobile Computing, S. 195-231.

[88] Royer / Toh, 1999.

ten ist Jini[89], eine von Sun Microsystems entwickelte Technologie. Jini stellt Mechanismen bereit, um Geräte und Services dynamisch im Netz anzumelden, zu suchen und auch wieder abzumelden. Es liefert außerdem ein gemeinsames Schnittstellenmodell für Programmierer, um die Kommunikation zwischen Geräten einfacher zu handhaben. Jini basiert auf der objektorientierten Programmiersprache Java.

Wichtige Bestandteile der Architektur sind die eigentlichen Dienste selbst, z.B. Datenspeicherung, Berechnung, nutzbare Kommunikationskanäle. Es gibt einen Suchdienst (Lookup Service“), der zum Auffinden und Registrieren von Diensten dient. Das Sicherheitsmodell von Jini kennt zwei zentrale Konzepte, den Prinzipal (Principal, Auftraggeber eines Zugriffs, meist ein Nutzer) und Zugriffslisten (Access Control List) für ein Objekt oder einen Dienst. Der Zugriff auf einen Dienst ist zeitbeschränkt und wird zwischen Anbieter und Nutzer ausgehandelt; der Nutzer erhält ein befristetes Nutzungsrecht (Lease).

Obwohl sich Jini kommerziell nicht durchgesetzt hat, erscheinen manche der aufgezeigten Ansätze für eine Dienstarchitektur zwischen dynamisch vernetzten Objekten wegweisend.

Ähnliche Konzepte[90] finden sich zum Beispiel im „Service Location Protocol“ (SLP)[91], dem „Service Discovery Protocol“ (SDP) von Bluetooth, ZeroConf[92] und „Universal Plug and Play“ (UPnP)[93].

1.5.4.2 Das EPC-Netzwerk

Die RFID-Technologie soll standardmäßig durch ein umfangreiches Netzwerk an Internet-Servern ergänzt werden, das so genannte EPC-Netzwerk[94], um einen globalen und dynamischen Informationsaustausch über Objekte zu ermöglichen. Dieses Netzwerk wird nicht auf den eigentlichen Chips implementiert werden, ist also nicht eine höhere Protokollschicht, die etwa auf RFID als Bitübertragungs- und Sicherungsschicht aufbaut. Es handelt sich vielmehr um eine Art „Meta“-Netzwerk zur Gewinnung, Speicherung und Verbreitung von Informationen über die mit Chips versehenen Gegenstände.

Zentraler Akteur ist das Standardisierungskonsortium EPCglobal[95], das ein Joint Venture von EAN International (jetzt GS1) und Uniform Code Council (UCC) darstellt. Entwickelt wurde das EPCglobal Netzwerk zuvor von den Auto-ID Labs, einem globalen Forschungsteam unter Leitung des Massachusetts Institute of Technology (MIT).

Voraussetzung für das EPC-Netzwerk ist, alle interessanten Objekte (zum Beispiel Einzelar-

---

[89] Jini Homepage: http://www.jini.org/ (30.03.2006); Roth, op. cit., S. 237ff.

[90] Roth, op. cit., S. 231-243.

[91] RFC 2165; RFC 2608.

[92] Zero Configuration Networking (Zeroconf): http://www.zeroconf.org/ (30.03.2006).

[93] UPnP-Forum: http://www.upnp.org/ (30.03.2006).

[94] EPC steht für „Electronic Product Code“ und ist der Nachfolger des Barcodes, allerdings mit eindeutigen Seriennummern, siehe die folgenden Ausführungen.

[95] EPCglobal: http://www.epcglobalinc.com (30.03.2006).

tikel im Handel) mit einem RFID-Funkchip (Tag) auszustatten, der über eine Luftschnittstelle mit Lesegeräten (Reader) kommuniziert. Tags und Lesegeräte zusammen bilden ein so genanntes ID-System.

Im Sinne des Standards enthält jeder RFID-Tag eine global eindeutige Nummer, den so genannten Electronic Product Code (EPC). Dieser EPC fungiert in Erweiterung des herkömmlichen Barcodes als eindeutige Identifikationsnummer für jedes einzelne physikalische Objekt, das einen Funkchip trägt.

Nach dem Auslesevorgang leiten die Lesegeräte den EPC weiter an eine Middleware, die wiederum mit Hilfe von Namens- und Informationsdiensten wie dem Object Name Service (ONS) und dem EPC Discovery Service weiterführende Serveradressen für den EPC in Erfahrung bringt.

Auf diesen weiterführenden Servern, die man auch als EPC Information Server (EPCIS) bezeichnet, sind die eigentlichen Zusatzinformationen zum jeweiligen Objekt zu finden, zum Beispiel zu Ort und Zeitpunkt seiner Produktion, Auslieferstatus oder Verkaufsdatum.

Mit seinem Ansatz, Daten nicht auf den Tags, sondern auf verteilten Hintergrundsystemen zu speichern (Paradigma: „Data on Network"), könnte sich das EPC-Netzwerk vom ursprünglichen Einsatz in der Logistik zu einem globalen Informationsspeicher und –vermittler für UC-Umgebungen weiterentwickeln, die RFID einsetzen, um Objekte zu identifizieren, und anhand des EPC zusätzliche Informationen für die weitere Dienstbereitstellung einholen.

1.5.4.3 Location-based Services

Location-based Services (LBS) sind eine Familie von möglichen Diensten auf der Anwendungsschicht, die einerseits die genaue Position des Nutzers berücksichtigen, technisch aber auch aus der Ferne angeboten werden können. Man kann LBS als Dienste definieren, die Daten über den Aufenthaltsort eines Gerätes zusammen mit anderen Informationen nutzen, um einen Mehrwert für den Nutzer herzustellen. Zur Nutzerlokalisierung können z.B. GPS oder lokale drahtlose Netze wie WLAN genutzt werden. Bei genügend hoher Dichte an Lesegeräten kann auch RFID zum Einsatz kommen. Schon nach Definition erlauben LBS ein „Tracking" von Nutzern, d.h. das systematische Feststellen des Aufenthaltsorts und die Verfolgung ihrer Bewegung.

Ein dreischichtiges Modell kann zur Beschreibung von LBS genutzt werden.[96] Die Grundlage bildet ein „Positioning Layer", der die Positionsbestimmung eines Gerätes oder Nutzers mittels eines geographischen Informationssystems (GIS) durchführt. Eine Middleware vermittelt zwischen den Schichten der Positionierung und der eigentlichen Anwendung und dient einer einfacheren Realisierung der Schnittstellen zwischen diesen Schichten.

LBS lassen sich hauptsächlich in drei Bereichen einsetzen: Militär und Behörden, Rettungsdienste und für kommerzielle Angebote. Beispiele für kommerzielle Nutzung sind „Tracking"

[96] Spiekermann, General Aspects of Location-Based Services, 2004.

z.B. von Kindern, Haustieren, Besitztümern und Autos, Flottenmanagement, Navigation, Kommunikation, Tourismusinformation, lokale Werbung, Gaming und Entertainment. Unterschieden werden personenorientierte und geräteorientierte Dienste, wobei meist nur bei den erstgenannten die lokalisierte Person oder das Gerät Kontrolle über den Dienst ausüben kann.

Eine andere Einteilung ist die nach der Initiative beim Nutzen des Dienstes: „Push" vs. „Pull" Services. Bei „Push"-Diensten werden dem Nutzer ohne sein aktives Mitwirken spezielle und möglicherweise individualisierte Angebote von außen gewissermaßen aufgedrängt. Bei „Pull"-Diensten dagegen initiiert der Nutzer die jeweilige Interaktion aktiv und aus eigenem Antrieb, zum Beispiel durch ortsbezogene Suchanfragen.

Mit zunehmender Durchdringung des Alltags mit eingebetteten oder mobilen Rechnern bieten sich gesteigerte Einsatzmöglichkeiten für LBS. Die Nutzerlokalisierung kann durch verschiedene Accesstechnologien genauer werden, und es bieten sich neue Ansprechmöglichkeiten durch neuartige und ubiquitäre Mensch-Computer Schnittstellen (HCI, „Human-Computer Interfaces").

1.6 Mensch-Computer Interaktion

Mensch-Computer Interaktion (Human-Computer Interaction, HCI)[97] ist ein interdisziplinäres Forschungsgebiet, das sich mit der Entwicklung, Gestaltung, Untersuchung und Implementierung interaktiver Computer-Systeme für den menschlichen Gebrauch und mit der Erforschung der in diesem Bereich auftretenden Phänomene auseinandersetzt.

Eine allgemein akzeptierte und trennscharfe Definition des Themenbereichs, der HCI ausmacht, existiert nicht. Bei der Gestaltung der Schnittstellen, die die Interaktion ermöglichen, sind neben der grundlegenden Hard- und Software insbesondere auch die Gebiete z.B. der künstlichen Intelligenz, Ergonomie, Kommunikations-Design, Psychologie oder Soziologie wichtige Forschungsbereiche. Ziel ist die Gestaltung einer als intuitiv oder natürlich bezeichneten Bedienbarkeit von Computern, damit Nutzer sich nicht für jedes Gerät zunächst ein neues Interaktions-Paradigma aneignen müssen. So soll nicht nur die Effektivität der Nutzung gesteigert werden, sondern die Nutzung von Computern auch Menschen ohne technisches Know-how ermöglicht werden.

Die Gestaltung derartiger Schnittstellen ist ein grundlegender Baustein für Ubiquitous Computing.[98] Gleichzeitig ist die HCI-Entwicklung auf Ergebnisse aus den anderen aufgezeigten Bereichen, z.B. verbesserte Sensorik und Auswertungsmethoden ebenso wie neue Ausgabemedien, angewiesen, um den Nutzern situationsangepasste Interaktionsmöglichkeiten anzubieten.

---

[97] ACM SIGCHI Curricula for Human-Computer Interaction: http://www.acm.org/sigchi/cdg/cdg2.html (30.03.2006); Interaction-Design.org: http://www.interaction-design.org/ (30.03.2006); Laurel (Ed.), The Art of Computer Interface Design, 1990; Raskin: The Humane Interface, 2000; Shneiderman / Plaisant: Designing the User Interface, 2004

[98] Lipp: Interaktion zwischen Mensch und Computer im Ubiquitous Computing, 2004.

1.7 Zusammenfassung

1.7.1 Konvergenz zu IP

Eine sehr zentrale technische Tendenz ist die Konvergenz der meisten Kommunikationstechniken zu IP-basierten Netzwerken. So hat man früher Modems ("IP-über-Telefon") benutzt, um heutzutage VoIP ("Telefonie-über-IP") zu favorisieren. Analog ist eine Entwicklung zu IP als Netzwerkschicht über sehr heterogene Zugangstechnologien im Gange.

Speziell IPv6 bietet sehr flexible neue Mechanismen für die drahtlose, mobile Kommunikation und mit dem gewaltigen Adressraum auch die Möglichkeit, alle Geräte der ubiquitären Umgebungen aus der Ferne zu adressieren.

1.7.2 Datenfluss im Ubiquitous Computing

Ubiquitous Computing zeichnet sich durch eine neue Phase in der Quantität vernetzter Objekte in unserem Alltag aus. Ferner ergibt sich auch ein neuer Maßstab in der Quantität und Qualität gespeicherter Daten, die das einzelne Individuum betreffen.

Als Beispiel für den Datenfluss und die Informationsspeicherung in ubiquitären Systemen soll die folgende Darstellung eines kleinen Ausschnittes einer möglichen zukünftigen Netzlandschaft dienen. Mobile Entitäten (Menschen, Tiere, Fahrzeuge oder Maschinen) führen ein enges Body Area Network (BAN) auf ihrer Oberfläche mit sich, ferner umgibt sie ein etwas weiter reichendes Personal Area Network (PAN). Diese eher persönlichen Geräte speichern Daten und Profile des Nutzers, sie enthalten Sensoren und eventuell auch Aktuatoren, die aus der Ferne kontrollierte Bewegungen auslösen können.

Geräte aus den BANs und PANs verschiedener Entitäten können Ad-hoc-Netzwerke miteinander bilden, Daten mit der lokalen Infrastruktur austauschen (in der Abbildung bezeichnen alle schwarzen Pfeile einen bidirektionalen, transitiven Datenfluss) oder von dieser mithilfe von Sensornetzen z.B. optisch oder mittels RFID erfasst, lokalisiert und identifiziert werden (weiße Pfeile). Mittels GPS oder anderer Lokalisierungssysteme können die Entitäten selbst ihre aktuelle Position bestimmen. Je nach der Infrastruktur in Reichweite greifen die Entitäten über das lokale Netz (LAN), das Metropolitan Area Network (MAN) – z.B. via WiMAX – oder über Mobilfunk auf das Internet zu oder sind prinzipiell auch über alle Wege unter einer festen IPv6-Adresse erreichbar. Wiederum fallen jeweils Datenspuren in der Infrastruktur an.

Schließlich kann auf entfernte Dienste (Remote Services) im Internet zugegriffen werden, oder entfernte Service Provider können umgekehrt über die verschiedenen Verbindungswege auf die lokalen Geräte im jeweiligen LAN, BAN und PAN zugreifen und in Wechselwirkung treten. Somit ergibt sich auch eine entfernte Datenhaltung auf möglicherweise zahlreichen und global verteilten Servern.

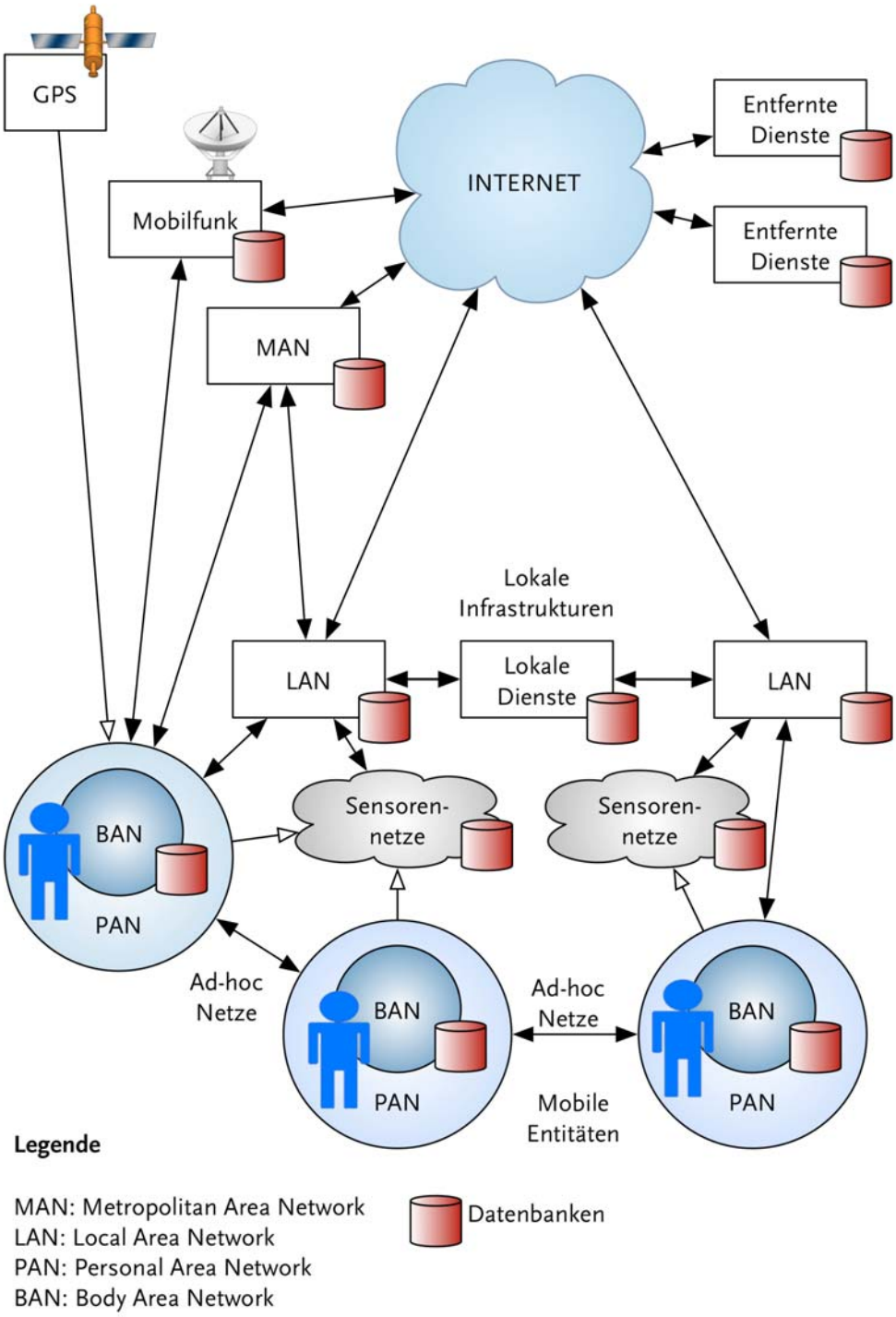


Abbildung 5: Datenfluss im Ubiquitous Computing

Da im Ubiquitous Computing detaillierte Personenprofile Grundlage vieler Anwendungen sind, müssen Lösungen erarbeitet werden, die eine nutzerfreundliche Wahrnehmung des Rechts auf informationelle Selbstbestimmung ermöglichen und sicherstellen, dass keine Dritten Zugriff auf die sensiblen Daten nehmen können.

1.8 Literatur

Abowd, Gregory D. / Mynatt, Elizabeth D.: Charting Past, Present, and Future Research in Ubiquitous Computing, ACM Transactions on Computer-Human Interaction, Vol. 7, No. 1, März 2000, S. 29–58.

ACM SIGCHI Curricula for Human-Computer Interaction: http://www.acm.org/sigchi/cdg/cdg2.html (30.03.2006).

Adams Communications, Vergleich UPC/EAN: http://www.adams1.com/pub/russadam/upccode.html (30.03.2006).

Aliev, Rafik Aziz / Fazlohalli, Bijan / Aliev, Rashad Rafik: Soft Computing and its Applications in Business and Economics, Studies in Fuzzyness and Soft Computing, Vol. 157, Springer, Berlin, 2004.

Anderson, Ross: Security Engineering – A Guide to Building Dependable Distributed Systems, Wiley, New York, 2001.

Berners-Lee, Tim: Weaving the Web - The Past, Present and Future of the World Wide Web, Texere, London, 2000.

Berners-Lee, Tim, Semantic Web Roadmap, 1998, http://www.w3.org/DesignIssues/Semantic.html (30.03.2006).

Birman, Kenneth P.: Reliable Distributed Systems – Technologies, Web Services and Applications, Springer, 2005.

Bless, R. / Blaß, E.-O. / Conrad, M. / Hof, H.-J. / Kutzner, K. / Mink, S. / Schöller, M.: Sichere Netzwerkkommunikation, Springer, 2005.

Bluetooth Spezifikationen, https://www.bluetooth.org/spec/ (30.03.2006).

Bharatula, Nagendra / Ossevoort, Stijn / Stäger, Mathias / Tröster, Gerhard: Towards Wearable Autonomous Microsystems, 2004, http://www.wearable.ethz.ch/fileadmin/pdf_files/pub/pervasive04-bharatula.pdf (30.01.2006).

Boeker, Peter: Technisch-sensorische Geruchsmessung, Universität Bonn, 2004, http://www.landtechnik.uni-bonn.de/ifl_research/pp_3/Technisch-sensorische_Geruchsmessung_Kassel.pdf (30.03.2006).

BSI, Sicherheit im Funk-LAN (WLAN, IEEE 802.11): http://www.bsi.bund.de/literat/doc/wlan/ (30.03.2006).

Bundesamt für Sicherheit in der Informationstechnik (BSI): Risiken und Chancen des Einsatzes von RFID-Systemen, 2004, http://www.bsi.bund.de (06.03.2006).

Buse, Karsten: Optische Datenübertragung, Universität Bonn, http://pi.physik.uni-bonn.de/hertz/Papers/talks/041213KB.pdf (30.03.2006).

Cambridge University Computer Laboratory / AT&T: The Bat Ultrasonic Location System, http://www.cl.cam.ac.uk/Research/DTG/attarchive/bat/ (30.03.2006).

Chaos Computer Club zu GSM: http://www.ccc.de/gsm/ (30.03.2006).

Chappell, David / Jewell, Tyler: Java Web Services, O'Reilly, Köln, 2003.

Digital Voices Projekt: http://www.ics.uci.edu/~lopes/dv/dv.html (30.03.2006).

Eckert, Claudia: IT-Sicherheit, Oldenbourg Verlag, 3. Auflage, 2004.

EPCglobal: EPC Radio-Frequency Identity Protocols – Class-1 Generation-2 UHF RFID, 2004.

EPCglobal RFID Standards: http://www.epcglobalinc.com/standards_technology/specifications.html (30.03.2006).

ETSI HIPERLAN/2 Standard: http://portal.etsi.org/radio/HiperLAN/HiperLAN.asp (30.03.2006).

Finkenzeller, Klaus: RFID-Handbuch, Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 3. Auflage, Hanser Verlag, München/Wien, 2002.

Fleisch, Elgar / Mattern, Friedemann (Hrsg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, Springer, 2005.

Fraunhofer ISC: http://www.isc.fraunhofer.de/german/geschaeftsfelder/gf4/ (30.03.2006).

GALILEO Projekt: http://europa.eu.int/comm/dgs/energy_transport/galileo/index.htm (30.03.2006).

Garfinkel, Simson / Rosenberg, Beth (Hrsg.): RFID Applications, Security, and Privacy, Addison-Wesley, 2005.

GLONASS: http://www.glonass-center.ru/frame_e.html (30.03.2006).

Greenberg, Eric: Network Application Frameworks – Design and Architecture, Reading, 1999.

GSM Association: http://www.gsmworld.com/index.shtml (30.03.2006).

Hagen, Silvia: IPv6 Essentials, O'Reilly, Sebastopol, 2002.

Hagino, Jun-ichiro itojun: IPv6 Network Programming. Amsterdam/Boston, 2005.

Hansen, Marit / Wiese, Markus: RFID – Radio Frequency Identification, DuD - Datenschutz und Datensicherheit, 28, 2, 2004, S. 109.

Hilty, Lorenz / Behrendt, Siegfried / Binswanger, Mathias / Bruinink, Arend / Erdmann, Lorenz / Fröhlich, Jürg / Köhler, Andreas / Kuster, Niels / Som, Claudia / Würtenberger, Felix: The Precautionary Principle in the Information Society – Effects of Pervasive Computing on Health and Environment. EMPA, Bern, 2005, http://www.empa.ch/sis (17.03.2006).

Hurman, Tim / Rowe, Mark: Bluetooth Security - Issues, threats and consequences, WBF2004, Cambridge, http://www.pentest.co.uk/documents/wbf_slides.pdf (30.03.2006).

IBM Think Research: The Body Electric, http://domino.research.ibm.com/comm/wwwr_thinkresearch.nsf/pages/pan197.html (30.03.2006).

IBM PAN Fact Sheet: http://www.almaden.ibm.com/cs/user/pan/pan.html (30.03.2006).

IEEE 802.11 Standards: http://standards.ieee.org/getieee802/ (30.03.2006).

IEEE 802.15 WPAN Task Group, http://ieee802.org/15/pub/TG4.html (30.03.2006).

IEEE 802.16 Working Group: http://ieee802.org/16/ (30.03.2006).

IETF, Request for Comments (RFC) Reihe, z.B. unter: http://www.rfc-editor.org/ (30.03.2006).

Ilyas, Mohammad (Hrsg.), The Handbook of Ad Hoc Wireless Networks, Boca Raton/London, 2003.

InterVal Projekt der HU Berlin: http://interval.hu-berlin.de/rfid/ (30.03.2006).

Infrared Data Association (IrDA): http://www.irda.org/ (30.03.2006).

Interaction-Design.org: http://www.interaction-design.org/ (30.03.2006).

ISO Standard zum ISO/OSI-Modell: ISO/IEC 7498-1:1994.

ISTAG - IST Advisory Group: Ambient Intelligence - From Vision to Reality, 2003, ftp://ftp.cordis.lu/pub/ist/docs/istag-ist2003_consolidated_report.pdf (30.03.2006).

Jini Homepage: http://www.jini.org/ (30.03.2006).

JXTA Projekt: http://www.jxta.org/ (30.03.2006).

Kranz, Matthias: Sensoren, Microcontroller und Ubiquitous Computing, 2004, http://www.hcilab.org/matthias/SensorenMicrocontrollerUbiquitousComputing.pdf (30.03.2006).

Laurel, Brenda (Hrsg.), The Art of Computer Interface Design, Addison-Wesley, 1990.

Lauterwasser, Christoph: Opportunities and Risks of Nanotechnologies - Report in co-operation with the OECD International Futures Programme, München, 2005, http://www.allianz-azt.de/azt.allianz.de/Industrietechnik/Content/Downloads/Files/Nanotech_dotcom3mb.pdf (Stand: 30.03.2006).

Lipp, Lauritz L.: Interaktion zwischen Mensch und Computer im Ubiquitous Computing, LIT, Münster, 2004.

Loshin, Peter: IPv6 Theory, Protocol and Practice, 2nd ed., Boston, 2004.

Lopes, Cristina / Aguilar, Pedro: Acoustic Modems for Ubiquitous Computing, IEEE Pervasive Computing 2(3), Juli-September, 2003.

Löwer, Chris: Wer Böses plant, hat schlechte Karten, http://www.pm-magazin.de/de/heftartikel/artikel_id908.htm (15.11.2004).

Lyytinen, Kalle / Yoo, Youngjin: Issues and Challenges in Ubiquitous Computing, CACM 45(12), 2002. S. 62-65.

Marculescu, Diana / Marculescu, Radu / Zamora, Nicholas et al.: Electronic Textiles, A Platform for Pervasive Computing, 2003, http://www.wearable.ethz.ch/fileadmin/pdf_files/pub/Marculescu032.pdf (30.01.2006).

McCloskey, Paul: From RFID to a Smart World, Brussels 2004, ftp://ftp.cordis.lu/pub/ist/docs/directorate_d/ebusiness/mccloskey_en.pdf (30.01.2006).

OASIS Homepage zu UDDI: http://www.uddi.org (30.03.2006).

Pister, Kris / Kahn, Joe / Boser, Bernhard: Smart Dust – Autonomous Sensing and Communication in a Cubic Millimeter, http://robotics.eecs.berkeley.edu/~pister/SmartDust/ (30.01.2006).

RDF Spezifikation, http://www.w3.org/TR/PR-rdf-syntax/ (30.03.2006).

Raskin, Jef: The Humane Interface - New Directions for Designing Interactive Systems, Addison Wesley, 2000.

Rech, Jörg: Wireless LANs, 802.11-WLAN-Technologie und praktische Umsetzung im Detail, Heise Verlag, Hannover 2004.

Roth, Jörg: Mobile Computing – Grundlagen, Technik, Konzepte, Heidelberg 2002.

Royer, Elizabeth / Toh, Chai-Keong: A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, IEEE Personal Communications, April 1999, S. 46-55.

Sankar, Krishna / et al.: Cisco Wireless LAN Security, Indianapolis, 2005.

Satyanarayanan, M. (Hrsg.): Energy Harvesting & Conservation, IEEE Pervasive Computing, Vol. 4, No. 1, January-March 2005.

Schmidt, Albrecht : Ubiquitous Computing – Computing in Context, PhD Thesis, Lancaster 2002, http://www.comp.lancs.ac.uk/~albrecht/phd/index.html (30.03.2006).

Schiller, Jochen: Mobile Communications, 2nd Ed., Addison-Wesley, London/Boston, 2003.

Schoch, Thomas: Middleware für Ubiquitous-Computing-Anwendungen, in: Fleisch / Mattern (Hrsg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, 2005, S. 119-140.

Shneiderman, Ben / Plaisant, Catherine: Designing the User Interface – Strategies for Effective Human-Computer Interaction, 4th ed., Addison Wesley, 2004.

Soliman, Hesham: Mobile IPv6, Mobility in a Wireless Internet, Boston, 2004.

Spiekermann, Sarah: General Aspects of Location-Based Services, in Schiller, Jochen / Voisard, Agnès (Hrsg.), Location-based Services, San Francisco, 2004.

Spiekermann, Sarah / Ziekow, Holger RFID Technologie und Implikationen, Vortrag 2005, http://interval.hu-berlin.de/rfid/ (30.03.2006).

Stäger, Mathias / Lukowicz, Paul / Tröster, Gerhard: Implementation and Evalutation of a Low-Power Sound-Bases User Activity Recognition System, 2004, http://www.wearable.ethz.ch/fileadmin/pdf_files/pub/staeger_iswc04.pdf (30.01.2006).

Stajano, Frank: Security for Ubiquitous Computing, Wiley, Chichester, 2002.

Steinmetz, Ralf / Wehrle, Klaus (Hrsg.): Peer-to-Peer Systems and Applications, Springer, LNCS 3485, 2005.

Stevens, W. Richard: TCP/IP Illustrated, Volume 1 – The Protocols, Addison Wesley, 1994.

SWAMI Projekt – Safeguards in a World of Ambient Intelligence: http://swami.jrc.es/pages/ (17.03.2006).

Tamm, Gerrit / Günther, Oliver: Webbasierte Dienste, Physica / Springer, Heidelberg 2005.

Tandler, Peter: Software Infrastructure for Ubiquitous Computing Environments – Supporting Synchronous Collaboration with Heterogeneous Devices, Proceedings of UbiComp 2001, Springer, LNCS 2201, Heidelberg 2001, S. 96-115.

TEA Projekt: http://www.teco.edu/tea/tea_vis.html (30.03.2006).

Thoms, Henrik: Smart Dust, Weimar, 2003, http://www.uni-weimar.de/~heymann/Public/manet_maus.pdf (30.01.2006).

UCONN NOPP FRONT Projekt (Ozeanographie): http://www.nopp.uconn.edu/ADCP/ (30.03.2006).

ULD zu WLAN: http://www.datenschutzzentrum.de/material/tb/tb26/kap10.htm#Tz10.1 (30.03.2006).

UMTS Report: http://www.umts-report.com/umts.php (30.03.2006).

UPnP-Forum: http://www.upnp.org/ (30.03.2006).

Vault Information Services, Barcode Symbology: http://www.barcodeisland.com/symbolgy.phtml (30.03.2006).

Vladimirov, Andrew / Gavrilenko, Konstantin V. / Mikhailovsky, Andrei A.: WI-FOO – The Secrets of Wireless Hacking, Addison-Wesley, Boston, 2004.

Weiser, Mark: The Computer for the 21st Century, Scientific American, 265, 3, 1991, S. 66-75.

Weiser, Mark: Some Computer Science Problems in Ubiquitous Computing, CACM 36(7), Juli 1993. S. 75-84.

Weiser, Mark / Brown, John S.: The Coming Age of Calm Technology, 1996, http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm (06.03.2006).

Weiser, Mark: Ubiquitous Computing Homepage: http://www.ubiq.com/hypertext/weiser/UbiHome.html (30.03.2006).

Wikipedia Online Enzyklopädie: http://de.wikipedia.org/ (30.03.2006).

WiMAX Forum: http://www.wimaxforum.org/ (30.03.2006).

Zero Configuration Networking (Zeroconf): http://www.zeroconf.org/ (30.03.2006).

Zhang, Jianwei: Angewandte Sensorik, Universität Hamburg, 2003, http://tech-www.informatik.uni-hamburg.de/lehre/ws2003/vorlesungen/angewandte_sensorik/ (30.03.2006).

ZigBee Alliance, http://www.zigbee.org/ (30.03.2006).

2 Anwendungsfelder

Markus Hansen, Benjamin Fabian, Michael Klafft

2.1 Einleitung

Während eine vollständige Welt des Ubiquitous Computing (UC) noch Vision ist, gibt es Anwendungsfelder, in denen die in Kapitel 1 beschriebenen Techniken bereits heute zum Einsatz kommen oder ihre Einführung bereits so konkretisiert ist, dass sie in Kürze erwartet werden kann. In der Regel handelt es sich um geschlossene Systeme, die keine oder nur wenige Schnittstellen zu anderen Systemen haben.[99] Mit anderen Worten verläuft die Diffusion des Ubiquitous Computing aus innovationstheoretischer Sicht vermutlich stufenweise, von vielen Einzelanwendungen in eher geschlossenen Systemen hin zur Verwirklichung der Vision ihrer allgegenwärtigen Vernetzung. Im Folgenden werden die Anwendungsfelder skizziert, in denen bereits heute Ubiquitous Computing Wirklichkeit ist oder deren Einführung in Kürze bevorsteht.

2.2 Fahrzeugkontrollsysteme

Fahrzeuge bilden ein geeignetes Umfeld für den Einsatz von UC-Systemen, da sie einen begrenzten, gut definierbaren Raum darstellen sowie über eine autarke Energieversorgung verfügen.

Sensorsysteme - wie heute schon in Flugzeugen vorhanden - werden in Zukunft verstärkt in Automobilen für eine ständige Überwachung diverser Fahrzeugparameter sorgen. Beispiele sind Sensoren, die den Luftdruck der Reifen, den Abstand des Fahrzeuges zu seiner Umgebung, die Temperatur oder die Feuchtigkeit sowie die Helligkeit messen. Abhängig von den Messwerten werden im Fahrzeug von einem Kontrollsystem bestimmte Reaktionen ausgelöst, um es auf seine Umgebung einzustellen und sein Verhalten zu optimieren.

RFID wird schon seit längerem zur Zugangskontrolle in Autoschlüsseln verwendet. Die im jeweils verwendeten System eindeutige Kennung (ID) im Chip des Fahrzeugschlüssels dient dazu, den Fahrer an entsprechend ausgestatteten Tankstellen als registrierten Kunden auszuweisen. Die derart in Anspruch genommene Leistung wird bargeldlos abgerechnet.[100] Mit fortschreitender Entwicklung kann die Identifikation des Fahrers auch über biometrische Sensoren erfolgen. Zumindest als Konzeptstudien werden derartige Systeme bereits von Automobilherstellern vorgestellt.[101]

Die Speicherung der individuellen Präferenzen eines Fahrers ermöglicht es, das Fahrzeug

[99] Zur Problematik des Übergangs von geschlossenen zu offenen Systemen vgl. auch Kapitel 7.

[100] Diese Anwendung wird insbesondere in den USA praktiziert. Vgl. Heise Newsticker, Autoschlüssel mit unsicherem Schlüssel, http://www.heise.de/newsticker/meldung/55729 (25.05.2005).

[101] Bust, Friedhelm, Autodiebe hacken Finger ab, http://www.rifid.de/logbuch/index.php/2005/04/01/autodiebe-hacken-finger-ab/ (03.06.2005).

an den jeweiligen Nutzer anzupassen. Auf diese Weise können zum Beispiel die Einstellungen der Spiegel, der Sitzhöhe und Abstände, aber auch der Klimaanlage oder die Programmauswahl oder Lautstärke von Audiogeräten im Wagen automatisch an den jeweiligen Fahrer individuell angepasst werden. Im Bordrechner können solche Profile auch für Dritte angelegt werden, die das Fahrzeug mitbenutzen oder denen es zeitweise überlassen wird. Einstellen lassen sich auch andere Funktionen wie eine Begrenzung der Geschwindigkeit oder der Fahrzeit. Auf diese Weise können auch am jeweiligen Fahrer (etwa Kategorie „Anfänger") orientierte Nutzungsbedingungen wie bspw. eine zulässige Maximalgeschwindigkeit eingestellt und automatisch durchgesetzt werden. Umgekehrt können Geschwindigkeitskontrollen oder eine Analyse von Auffälligkeiten im Fahrverhalten wie eine „schlenkernde" Fahrweise mittels Sensoren online vorgenommen werden. Über auf den Fahrer ausgerichtete Kameras können Abweichungen von seinem Normalfallverhalten wie bspw. das plötzliche Schließen der Augenlieder automatisch erfasst werden. Durch ein Warnsignal kann der Fahrer alarmiert und nebenbei das Signal auch an eine Kontrollinstanz übermittelt werden. Interessant sind derartige Anwendungen für den Arbeitgeber eines LKW-Fahrers, aber auch für Mietwagenfirmen oder Versicherungen. Letztere könnten ihre Entgelte dynamisch an die Risiken des individuellen Fahrverhaltens anpassen.[102] Bereits im Testeinsatz sind elektronische Fahrzeugschlüssel, die ein Atemtestgerät enthalten, so dass in Abhängigkeit vom festgestellten Alkoholwert ein Fahren verweigert werden kann.[103]

Es werden bereits heute Systeme zur Routenplanung (z.B. mittels GPS) ohne größeren Aufwand in Fahrzeuge integriert. Im Fahrzeug verfügbar sind leicht zugängliche Interfaces für die Mobilkommunikation und den Internetzugang (z.B. via UMTS oder in Zukunft auch WiMAX), die seine Vernetzung erleichtern.[104] Ein Vorreiter ist der Motorsport. So werden in der Formel 1 die am Auto gemessenen Systemparameter per Funk an das Service-Team übermittelt, um auf dieser Basis Entscheidungen über die Renntaktik zu treffen. Einer mobilen Überwachung über GPS unterliegen bereits heute LKW im Frachtbereich, um einerseits die Einsatzplanung über die Zentrale optimieren zu können, andererseits aber auch zur Diebstahlssicherung von Fahrzeugen und ihrer Fracht sowie zur Überwachung von Transportbedingungen[105]. Entsprechendes gilt für den Schiffsverkehr.

Die genaue Ortung der Fahrzeuge wird durch den Einsatz kombinierter Lokalisierungstechnologien in Zukunft immer leichter möglich werden. Bereits heute gibt es Fahrzeugsysteme, die beim Verlassen eines bestimmten Bereiches oder auf ein per Funk empfangenes Kom-

[102] Lypen, John, MOTOR Magazine 2001, Editor's Report, http://www.motor.com/MAGAZINE/articles/082001_03.html (16.04.2005).

[103] AutoWeb, Saab Develops ‚Alcokey' Breathalyser, http://autoweb.drive.com.au/cms/A_101770/newsarticle.html (15.06.2004).

[104] Für Flugzeuge siehe z.B.: Detlef Borchers, Surfen über den Wolken, c't, 11/2005.

[105] Trotec, Mobile Fernüberwachung in der Kühllogistik und Kältetechnik, http://www.trotec.de/pushcontent/data/00047.html (08.06.2005).

mando hin eine Wegfahrsperre aktivieren.[106] So soll Fahrzeugdiebstählen begegnet werden. Während Autos derzeit noch eher im Ausnahmefall während der gesamten Fahrt online sind, was eine externe Nutzung der Daten interner Sensoren ermöglichen würde, ist mit den Mautbrücken auf bundesdeutschen Autobahnen bereits ein für eine flächendeckende Überwachung geeignetes Netz fahrzeugexterner Sensoren installiert und im Einsatz.

Ferner erweitert sich die Verkehrsflussinformation auf öffentlichen Straßen um unzählige direkte Staumelder in Form entsprechend programmierter und vernetzt kommunizierender Sensorik innerhalb der Karosserie von Personen- und Lastkraftwagen. Die erfassten Datensätze könnten unter Verwendung harmonisierter Kommunikationsstandards zum Beispiel einem entgegenkommenden Fahrzeug zugefunkt werden. Mit diesen Informationen versehen errechnet ein Bordcomputer in Verbindung mit einem elektronischen Verkehrsinformationssystem Umleitungen und Ausweichmöglichkeiten.[107] In einem weiteren Entwicklungsschritt könnten Verkehrsleitsysteme[108] und Autopiloten in Zukunft zumindest auf Teilstrecken der Autobahnen die Lenkung von Fahrzeugen übernehmen. Sofern in allen am Straßenverkehr teilnehmenden Fahrzeugen ein System zum Austausch der Informationen über Position, Richtung und Geschwindigkeit mit anderen Fahrzeugen in der näheren Umgebung installiert ist, erlaubt dies Verkehrskonzepte, die z.B. ohne das zeitweise Anhalten einer kompletten Achse an Kreuzungen auskommen, indem die Fahrzeuge ihre Geschwindigkeiten so einander anpassen, dass die Verkehrsströme beider Achsen in Koordination gleichzeitig die Kreuzung passieren können.

Die zunehmende Vernetzung von Fahrzeugkomponenten[109] und ihr Datenaustausch mit anderen Nutzergeräten z.B. über Bluetooth[110] könnte zukünftigem „Mobilen Code“[111] die Ausbreitung über Systemgrenzen hinweg (z.B. vom PDA zur Autoelektronik) erlauben. Eine solche Entwicklung stellt potentiell eine Gefahr für die physische Sicherheit der Insassen sowie ihre Informationssicherheit dar. Schafft es ein Angreifer, Code auf ein Fahrzeugsystem einzuschleusen, kann er ggf. dort vorhandene Daten wie die Fahrerprofile einsehen oder Parameter zur Steuerung von Ereignissen wie das Auslösen des Airbags ändern, falls diese Systeme miteinander vernetzt sind.

---

[106] Dotinga, Randy, Wired News, http://wired-vig.wired.com/news/technology/0,1282,56536,00.html?tw=wn_story_related (03.01.2003).

[107] Vgl. das Konzept von *„floating car data“,* in Coroama, et al. 2003, 82 ff., S. 90.

[108] BMBF, Das intelligente und effiziente Verkehrsnetz. Leitprojekt Mobilität in Ballungsräumen, http://www.bmbf.de/de/637.php (25.05.2005).

[109] BMBF, Projekt „Mobiles Internet“, http://www.bmbf.de/de/mobilesinternet.php (25.05.2005).

[110] Beispiel ist die Planung einer universellen Kommunikations-„Black Box“ unter „Windows Automotive“, http://www.microsoft.com/industry/automotive/default.mspx (25.05.2005).

[111] Heise Security, Viren für Automobile noch keine Bedrohung, http://www.heise.de/security/news/meldung/56191 (09.02.2005).

2.3 Das Intelligente Haus

Bereits heutzutage existieren erste Pilotprojekte, um mit Hilfe von Ubiquitous Computing eine Wohnumgebung zu gestalten.[112] Beispiele sind das T-Com-Haus[113], Futurelife[114], In-Haus[115] oder das Gator Tech Smart-House[116]. Die Basis dieser Gestaltung ist die Vernetzung unterschiedlicher Objekte, deren Funktionen durch eine Person automatisch ausgelöst werden, indem sie als Individuum erkannt, sowie ihr Zustand und ihr Verhalten durch Sensoren erfasst werden. Ein Beispiel für eine solche Vernetzung ist das Zusammenspiel zwischen dem klingelnden Wecker und Funktionen wie dem Dimmen des elektrischen Lichtes, dem Öffnen der Gardinen, dem Anschalten der Heizung oder dem Aktivieren der Kaffeemaschine. Durch eine entsprechende Vernetzung könnte man die Hausklingel auch über ein Mobiltelefon hören oder das Klingeln des Telefons würde automatisch die Lautstärke der HiFi-Anlage senken. Individuell ausgelöst werden diese Funktionen aber erst, wenn Sensoren eine Person erkennen und eine kontextsensitive Entscheidungslogik die von dieser Person regelmäßig gewünschten Umgebungseinstellungen mit den aktuellen Erfordernissen in Verbindung bringt.

Teil einiger UC-Szenarien ist auch, dass die Wohnung zu einer individuellen Bilderwelt wird, in der in Bilderrahmen, auf Wänden oder in Spiegeln Videobotschaften, Filme, Bilder oder Texthinweise erscheinen, die von einer bestimmten Person oder einem bestimmten Situationskontext automatisch ausgelöst werden, wenn z.B. ein Raum betreten oder zu einer bestimmten Uhrzeit ein Sessel benutzt wird. Durch entsprechende Auslöser lassen sich auch individuell und zielgerichtet die Raumsituation wie beispielsweise die Fußboden- und Wandbeschaffenheit und -farbe gestalten sowie die Bedingungen des Wohnumfeldes nach den individuellen Voreinstellungen von der Beleuchtung bis zur Musik automatisch einstellen.

Die automatisierte und sich an Außentemperaturen anpassende Steuerung einer Heizungsanlage ist bereits heute Stand der Technik. Ubiquitous Computing erlaubt darüber hinaus eine Steuerung der auf einzelne Bewohner individuell und bedarfsgerecht eingestellten Temperatur- und Feuchtigkeitsverhältnisse in der Wohnung. Entsprechend kann auch die Umgebung des Hauses, z.B. Markisen, robotische Rasenmäher oder Bewässerungsanlagen, über eine automatische Steuerung gestaltet werden, die etwa bei einer bestimmten Temperatur, einer spezifischen Graslänge oder bei Trockenheit des Bodens ausgelöst wird.[117] Vernetzen – und damit auch automatisch ansteuern – lassen sich praktisch alle Ob-

[112] Für einen generellen Überblick siehe z.B. BSI 2002, für aktuelle Publikationen zum Thema „Smart Home“ vgl. VDI/VDE-IT online, http://www.vdivde-it.de/smarthome/publikationen.html (26.05.2005).

[113] T-Com Haus, http://www.t-com-haus.de/ (07.02.2006).

[114] Futurelife, //www.futurelife.ch/ (20.03.2005).

[115] InHaus-Innovationszentrum, Intelligente Raum- und Gebäudesysteme, http://www.inhaus-duisburg.de/ (20.03.2005).

[116] Gator-Tech Smart House, http://www.icta.ufl.edu/gatortech/index2.html (02.05.2005).

[117] Vgl. Bager, c't - Magazin für Computertechnik, 17, 2001, S. 114.

jekte in einer Wohnung. Anwendungen sind die Steuerung der Kochplatte über das Mobiltelefon oder Internet, um mit dem Kochen eines vorbereiteten Gerichtes zu einem festgelegten Zeitpunkt zu beginnen oder zu enden. Eine im Herd integrierte Waage kann das Gewicht der zu kochenden Ware selbstständig bestimmen, um dann die erforderliche Garzeit zu errechnen und an die Kochplatte weiterzureichen. Entwickelt werden weiterhin Roboter, die einfache Bringdienste und sogar Pflegeaufgaben übernehmen können.[118]

Ein portables Gerät oder im Haus verteilte Touchscreens (*„magic wand for the home"*[119]) erlauben als Fernbedienung den Zugriff auf Wohnraum-, Küchen- und Sanitätsgegenstände. Ein durchgängiges Sicherungssystem kontrolliert selbstständig die Ver- und Entriegelung aller verschließbaren Bereiche. Das Zutrittskontrollsystem kann zudem über verschiedene Interfaces (z.B. WAP, WWW) gesteuert werden. Eingangsbereiche mit moderner Sensortechnik identifizieren die Personen, die die Wohnung betreten wollen, an Hand von Transpondern oder biometrischer Merkmale und gestatten oder verweigern je nach Berechtigung den Zutritt.

Weiterhin erlaubt UC Anwendungen, die die individuellen Bedürfnisse seniorer oder auch behinderter Personenkreise zu erfüllen suchen. Automatisch lässt sich der Rollstuhl an das Bett steuern, das motorisierte Schlafbett bewegen oder das Fenster öffnen. Auf Bildern, Spiegeln und Wänden können die Wohnungsinhaber an wichtige Aufgaben erinnert werden. Auch könnte sich das Wohnumfeld an den jeweiligen Gemüts- und Gesundheitszustand anpassen, weil es über eine entsprechende Kamera- und Wahrnehmungssensorik verfügt.[120]

Die Kommunikations- und Steuerungstechnik in der Wohnung beschränkt sich nicht nur auf die eigentlichen Bewohner, sondern sie kann auch Nachrichten nach außen vermitteln oder einen Fernzugriff von außen ermöglichen. Private Sicherungs- und Alarmsysteme können ferngesteuert und an ein externes Sicherheitsunternehmen angebunden werden. Die elektronische Vernetzung einzelner Einrichtungen in der Wohnung ermöglicht die Fernwartung, eine Fehlerdiagnose oder gegebenenfalls auch online eine Reparatur von außen. So wird ein Gerätedefekt – beispielsweise einer Heiz- und Lüftungsanlage – automatisch eine Fehlermeldung an den Dienstleister auslösen und diesen mit den für eine Analyse erforderlichen Daten versorgen, die für die Vorbereitung eines ggf. notwendigen Einsatzes benötigt werden. Vor Ort kann sich der Handwerker dann mit den eigens für diese Reparatur zusammengestellten Werkzeugen und Ersatzteilen über ein mobiles Internetinterface (PDA) aktuelle Herstellerschaltpläne und Fachbedienungsanweisungen zu Nutze machen und eine effiziente Instandsetzung durchführen. Weiteres Beispiel ist die Verknüpfung der automatischen Erfassung des aktuellen Ölstandes einer Heizungsanlage mit der Ermittlung der aktuellen Preisangebote und Liefertermine über das Internet.

Ein anderes Beispiel für eine Kommunikation der Objekte innerhalb der Wohnung mit einem Dienstleister außerhalb ist die gezielte und automatische Versorgung mit Lebens- und

[118] Fraunhofer IPA, Care-O-Bot II, http://www.care-o-bot.de/Care-O-bot_2.php (08.06.2005).

[119] Helal et al., 2005.

[120] Vgl. Kuri, c't - Magazin für Computertechnik, 22, 1999.

Verbrauchsmitteln. So erlaubt ein in der Küche installierter Barcode- oder RFID-Scanner die Erfassung des aktuellen Warenbestandes und die Ermittlung des Fehlbestandes. Letztere werden ab einem bestimmten Schwellenwert automatisch an den Wohnungsinhaber zur Freigabe oder direkt an einen Dienstleister[121] übermittelt, der die erforderlichen Waren anliefert. Wird der Bestand an Waren und Verbrauchsgütern automatisch erfasst, dann können diese Informationen auch mit gezielten Informationen über Angebote und Lieferbedingungen über Internet oder andere Kommunikationsmittel wie das Fernsehen verbunden werden.[122]

2.4 Medizinische Anwendung

Eine bekannte Anwendung des Ubiquitous Computing im Medizinbereich ist die Ausstattung von Medikamentenpackungen mit RFID-Tags, über die jede einzelne Packung identifiziert werden kann. Eine solche Anwendung ermöglicht es, Zusatzinformationen über das Medikament wie Kontraindikationen und Haltbarkeit aus einer Datenbank abzurufen und zu nutzen. Die RFID-Tags sollen zudem helfen, gefälschte Medikamente (mit ggf. vom Original abweichender Zusammensetzung und Wirkung) als solche zu erkennen.[123]

Insbesondere im klinischen Bereich existieren bereits heute weitergehende Anwendungen. So gibt es im Bereich der medizinischen Logistik spezielle Behälter für Blutkonserven oder Laborproben[124], die Temperatursensoren und damit verbundene RFID-Tags enthalten, um die einzelnen Konserven oder Proben automatisiert identifizierbar zu machen. Ein integrierter Speicher für Temperaturwerte dient dazu, die unterbrechungsfreie Kühlkette nachzuweisen, die die Verwendungstauglichkeit des Blutes beeinflusst.

In Krankenhäusern ist es schon lange üblich, medizinisch wichtige Schlüsselwerte ständig zu überwachen und aufzuzeichnen. Während dies in der Vergangenheit noch über einzelne Apparate erfolgte, die neben dem Krankenbett aufgestellt wurden, Werte wie Körpertemperatur, Atmung oder Herzschlag erfassten und im Bedarfsfall über ein akustisches Signal das medizinische Personal alarmierten, wird diese Funktionalität zunehmend in das Bett integriert[125] und die Notfallbenachrichtigung über Kommunikationsdienste (z.B. Pager) vorgenommen werden.

---

[121] Vgl. zum Beispiel das von IBM und der britischen Supermarktkette Safeway entwickelte Bestellsystem „Easi-Order“: http://www-1.ibm.com/industries/retail/doc/content/bin/safeway.pdf (06.05.2005).

[122] Fragestellung dabei z.B., wie oft ein innerhalb eines vordefinierten Zeitrahmens nachweislich auf dem privaten audiovisuellen Ausgabemedium *X* mal umworbenes Produkt tatsächlich gekauft wurde.

[123] Computerwoche, Mit RFID gegen Viagra-Fälscher, http://www.computerwoche.de/index.cfm?artid=67648 (16.11.2004).

[124] Tagnology, Anwendungen Medizintechnik http://www.tagnology.com/anwendungen.asp?catIDMain=4&catIDSub=0&articleID=7 (26.05.2005).

[125] Institute for eGovernment, Das „intelligente“ Krankenhausbett, http://www.e-logo.de/html/modules.php?name=News&file=article&sid=2513 (26.05.2005).

Zudem können die Betten um zusätzliche Sensoren erweitert werden, die den physischen Zustand des Patienten wie z.B. sein Gewicht erfassen. Die anfallenden Daten lassen sich über einen lokalen Netzanschluss aus der Ferne abfragen und auswerten. Ebenfalls über das Netz lassen sich angeschlossene Geräte wie z.B. die Medikamentenzufuhr einer Tropfinfusion, Herzschrittmacher oder implantierte Insulinpumpen steuern und regeln. Wie in der Intensivmedizin lassen sich durch eine derartige automatisierte Erfassung der Patientendaten die jeweiligen Zustände und Entwicklungen zentral überwachen und nachvollziehen. Per Funk (z.B. WLAN) angebundene handliche Systeme mit Display bieten dem medizinischen Personal eine weitere Möglichkeit, mobil den Zustand ihrer Patienten zu überwachen.

Ein solcher automatisierter Zugriff auf Patientendaten wird nur einem hierzu autorisierten medizinischen Personal gewährt werden dürfen. Die Verwendung von RFID-Systemen zur Zugangskontrolle und Zeiterfassung kann die Identifizierung der berechtigten Personen sowie die Protokollierung ihrer Zugriffe vereinfachen, sofern geeignete Sicherheitsmechanismen entwickelt werden. Ein solches System ermöglicht es dem Personal, sich an beliebigen Terminals im Krankenhaus automatisiert anzumelden und von dort auf die gerade erforderlichen Daten der Patienten zuzugreifen und bestimmte Aktionen auszulösen.

Das Hintergrundsystem wird hierbei nicht nur die Erfassung der Patientendaten und den Zugriff auf diese steuern, sondern auch erfassen, wo sich welches Personal aufhält, um im medizinischen Notfall die Personen mit den im Einzelfall erforderlichen Qualifikationen an ihren Einsatzort zu rufen und auf diese Weise eine schnellst- und bestmögliche Versorgung der Patienten zu sichern.

Werden nun auch die Patienten mit Transpondern ausgestattet, ist bei einer entsprechenden Ausstattung der Klinik mit Lesegeräten auch deren jederzeitige Ortung möglich. Zusätzlich kann eine solche Identifikationsmöglichkeit die Gefahr verringern, dass Patienten miteinander verwechselt werden. Um die Eindeutigkeit einer solchen Markierung sicherzustellen, könnten Patienten mit subkutan implantierten RFID-Tags versehen werden. Im Zusammenspiel mit den beschriebenen mit RFID-Tags versehenen Medikamenten könnte nun bspw. die Ausgabe von Medikamenten automatisiert oder auf einem portablen System stets die Krankenakte des Patienten dargestellt werden.

In der Telemedizin gibt es Ansätze, Operationen fernzusteuern. Der Operateur sitzt an einem Bildschirm-Arbeitsplatz und bedient spezielle Roboter, die den eigentlichen Eingriff am Patienten durchführen. Die mit speziellen Sensoren ausgestatteten Roboter ermöglichen es dem Operateur, aktuelle Bedingungen und Veränderungen beim Patienten zu erkennen und entsprechend zu reagieren. Die Möglichkeit, andere Personen „hinzuzuschalten“, eröffnet die Durchführung spezieller Eingriffe, auch wenn der hierzu erforderliche Experte vor Ort nicht zur Verfügung steht. Auch kann die Operation per Video-Konferenzsystem übertragen werden, so dass weitere Personen an anderen Orten als Berater mitwirken oder zu Ausbildungszwecken die Operation verfolgen können.

Neben Einsatzfeldern im klinischen Bereich ist auch die ambulante Betreuung und Versor-

gung von Patienten ein Anwendungsbereich des Ubiquitous Computing.[126,127] So existieren Geräte, die auch außerhalb des Klinikums medizinisch relevante Daten von Patienten erfassen, auswerten und (z.B. per GSM-/UMTS-Netz) an Kliniksysteme oder Medizinisches Personal (z.B. Hausarzt) übermitteln. Ergibt die Auswertung eine Notfallsituation, kann automatisiert Hilfe angefordert werden. Ein derart alarmierter Notarzt kann mobil auf die medizinische Vorgeschichte des Patienten zugreifen oder mit dessen Hausarzt in Kontakt treten, um seine Entscheidungen auf einer fundierten Datenbasis zu treffen.

2.5 Warenwirtschaft und Logistik

In wenigen Bereichen ist der Einsatz von UC-Lösungen bereits so weit verbreitet wie in der Warenwirtschaft und der Logistik. Barcode- und RFID-basierte Identifikationssysteme ermöglichen hier die Rückverfolgung von Containern, Paletten und Produkten und verbessern so die Transparenz in der Lieferkette. Verfolgt wird dabei die Vision einer Lieferkette, in der von den beteiligten Partnern jederzeit auf alle verfügbaren Informationen zugegriffen werden kann – und dies über den gesamten Produktlebenszyklus.[128] Die Erfassung und Bereitstellung von Daten über die Grenzen einer Unternehmung hinweg ermöglichte dabei einen Paradigmenwechsel in der Lieferprozesssteuerung. Zentral organisierte Prozesssteuerungsmechanismen wurden zunehmend durch dezentrale, stark an der tatsächlichen Nachfrage ausgerichtete Bestellmechanismen ersetzt. Erfolgte früher der Abruf neuer Waren im Rahmen von (wöchentlichen) Sammelbestellungen, so werden heute die Verkaufsinformationen am Point of Sale unverzüglich an die Lieferanten weitergegeben.[129] Diese Bereitstellung von Verkaufsstatistiken nahezu in Echtzeit ermöglicht ein optimiertes Bestandsmanagement – Sicherheitsbestände können reduziert und Bestellmengen an die tatsächlichen Gegebenheiten angepasst werden.

Um die Nachfrage in Zukunft noch genauer voraussagen und Lieferungen noch besser steuern zu können, werden derzeit Lösungsansätze erarbeitet, die die Informationserfassung nicht am Verkaufspunkt enden lassen, sondern darüber hinaus aktuelle Verbrauchsinformationen direkt beim Kunden sammeln. So wird beispielsweise über Kopiergeräte nachgedacht, die ihren Papier- oder Tonerstand online an entsprechende Papierbeschaffungs- und Papierversorgungsstellen übermitteln, die bei Bedarf ein Nachliefern und Nachladen veranlassen. Aktuelle Tintendrucker können der Treibersoftware bereits den Tintenstand der Patronen mitteilen und zum Teil statistische Verbrauchsdaten per Internet an die Hersteller übermitteln.

In den letzten Jahren wurde eine Reihe von Modellversuchen unternommen, bei denen

[126] Ein Beispiel ist die Idee eines Home Medical Advisor, vgl. Stajano, 2002, S. 51.

[127] Mobile Anwendungen in der Medizin: Big Brother hält gesund, Deutsches Ärzteblatt 99, Ausgabe 23 vom 07.06.2002, S. 22, http://www.aerzteblatt.de/v4/archiv/artikel.asp?id=31944 (26.05.2005).

[128] Vgl. Luckett, S. 51.

[129] Vgl. Doukidis und Pramatari, S. 573.

RFID-basierte Identifikationssysteme auch auf Einzelproduktebene zum Einsatz kamen.[130] Hiervon erhofft man sich aus Sicht der Logistik unter anderem folgende zusätzliche Vorteile:

- Verbesserter Schutz vor Schwund und Diebstahl;
- Reduktion und Identifikation von Fehlern im Lieferprozess (automatische Prüfung von Lieferungen auf Korrektheit und Vollständigkeit);
- unverzügliche Identifikation von Out-of-shelf-Situationen;
- Identifikation von Objekten und Abruf zugehöriger Materialinformationen im Rahmen des Produktrecyclings.[131]

Kombiniert man RFID-Technik mit entsprechender Sensorik, so lassen sich darüber hinaus für jedes individuelle Produkt qualitätsrelevante Transportparameter (zum Beispiel Temperatur, Feuchtigkeit, Erschütterungen etc.) erfassen und dokumentieren. Soll-Ist-Abweichungen werden auf diese Weise unverzüglich identifiziert, so dass Gegenmaßnahmen zeitnah eingeleitet und – im Schadensfalle – Verantwortlichkeiten leichter zugeordnet werden können.

Neben den beschriebenen Anwendungsfällen in der Distributionslogistik kommen UC-Lösungen auch in der Produktionslogistik zum Einsatz. Die digitale Kennzeichnung von Objekten bzw. Werkstückträgern eröffnet hier die Möglichkeit, maschinelle Bearbeitungsprozesse aufgrund von objektspezifischen Informationen automatisiert und dezentral zu koordinieren und zu steuern.[132] Die Produktionsplanung und -steuerung wird dabei von intelligenten Agenten übernommen, die zum Beispiel im Rahmen von „Agentenauktionen“ knappe Produktionsressourcen für ihren Fertigungsauftrag ersteigern.[133] Die Priorisierung der Produktionsaufträge erfolgt ad hoc vor Ort, was die Flexibilität und die Adaptivität des Produktionssystems signifikant erhöht. Auf diese Weise können UC-basierte Produktionssteuerungssysteme einen entscheidenden Beitrag zur Umsetzung der Vision einer kundenindividuellen Massenproduktion („Losgröße 1“) leisten.

2.6 Nahrungsmittel und Tierhaltung

Nach europäischem Recht[134] muss eine chargenbezogene Rückverfolgbarkeit von Lebensmittelprodukten gewährleistet werden. Besitzen diese Produkte eindeutige Identifikatoren z.B. in Form eines EPC auf einem RFID-Tag oder eines 2D-Barcodes, so können Aufsichtsbehörden mit entsprechenden Lesegeräten aus einer Datenbank die Herkunft und die durchlaufene Logistikkette eines Produktes unmittelbar abrufen. Auf diese Weise werden nicht nur

[130] Metro Future Store Initiative, http://www.future-store.org/ (29.03.2006).

[131] Vgl. Bohn et al. 2003, 26; Finkenzeller 2002, 291 f.; Hellweg, 2004; Posch / Epple, 2004, S. 17.

[132] Vgl. Vrba et al., 2005, S. 178.

[133] Vgl. Liu et al., 2004, S. 1042.

[134] Allgemein sieht VO 178/2002 EG die Rückverfolgbarkeit einzelner Chargen vor (noch nicht jedoch einzelner Produkte), Sondervorschriften für Rindfleisch: VO 1760/2000 EG, Eier: 1907/90 EWG, geändert durch VO 2052/03 EG, VO 2295/03 EG.

die gesetzlichen Rückverfolgbarkeitsanforderungen erfüllt[135], sondern es wird darüber hinaus ermöglicht, alle relevanten Informationen nahezu in Echtzeit zu ermitteln. So lassen sich im Falle von Beanstandungen Fehlerquellen schneller ermitteln und Rückrufaktionen zielgenauer durchführen.

Eine auf das einzelne Produkt bezogene Erfassung von Produktstatus und Frischegrad würde darüber hinaus eine Flexibilisierung des Haltbarkeitsmanagements ermöglichen.[136] Starr vorgegebene Haltbarkeitsdaten würden ersetzt durch eine Haltbarkeitsprognose, die der Verarbeitungs- und Transporthistorie des jeweiligen Produkts Rechnung trägt und laufend aktualisiert wird. So könnten der Vertrieb und die Verwertung von Lebensmitteln optimiert und Kosten in erheblichem Umfang gespart werden (Reduktion des Verderbs). Ob sich ein solches System in der Praxis durchsetzen kann, ist jedoch noch unsicher – hier besteht im Bereich der Lebensmittelsensorik noch Forschungs- und Entwicklungsbedarf.

Im Bereich der Tierhaltung ist eine eindeutige Markierung, die per Funk ausgelesen werden kann, bereits seit einiger Zeit Stand der Technik. Zuchttieren werden Transponder entweder in Form von Halsbändern oder als Ohrknopf verabreicht. Ebenfalls im Einsatz sind subkutan injizierbare kleine Glaskapseln[137], die RFID-Tags enthalten.[138] Die Markierungen dienen in der Zucht für Zwecke der Fütterung sowie der Stalllogistik, aber auch zur Seuchen- und Qualitätskontrolle[139]. Auch in der biologischen Forschung findet man Versuche, in denen Insekten eines Staates mit Transpondern gekennzeichnet wurden, um ihre Bewegungsmuster erfassen und analysieren zu können.[140] Zur Kennzeichnung von Haustieren sind RFID-Transponder in ersten Anwendungen zu finden. Bei gefährlichen Tieren wie „Kampfhunden" dienen sie als kontaktlose Erkennungs- und Warnsignal.[141] In Kombination mit einem Tierregister lassen sich über ein derartiges System entlaufene Haustiere orten und wiederfinden.[142]

---

[135] Hierzu würde theoretisch sogar ein Ordner mit den Lieferscheinen und Lieferrechnungen in papierbasierter Form genügen – was im Schadensfall einen langwierigen und aufwändigen Rechercheprozess in Gang setzt.

[136] Vgl. Li et al., 2005, S. 2f.

[137] Diese Variante ist wahrscheinlich nicht in der Tierhaltung zur Nahrungsproduktion einsetzbar. Lebensmittelhersteller ergreifen in ihrer Produktion aufwändige Schutzmaßnahmen, um Produktverunreinigung durch Glas bei der Verarbeitung zu vermeiden (gefordert zum Beispiel im International Food Standard).

[138] Finkenzeller, RFID-Handbuch, 2002, 376ff.

[139] Vergl. Kern & Wendl, 1997; Silicon.de: Die Kreditkarte wandert unter die Haut. Silicon.de ~ das Info-Netzwerk für IT und Business, 26.11.03, http://www01.silicon.de/cpo/_cfg/print.php?nr=12099 (27.08.2004).

[140] Universität Marburg, High-Tech-Ortung von Kleintieren, http://www.uni-marburg.de/zel/kleintier_radar_fotos_und_text.html (08.06.2005).

[141] Die Gefahr mangelnder Akzeptanz aufgrund akustischer Belästigung liegt auf der Hand. Dies ist ein Beispiel für ein System, das die menschliche Aufmerksamkeit – als knappe Ressource betrachtet – nicht schont.

[142] Siehe hierzu auch http://homeagainid.com/ und http://www.avidmicrochip.com/ (22.10.2004).

2.7 Dokumentensicherheit (Pässe)

Da sich z.B. mittels eines in ein Objekt eingebtteten RFID-Tags zusätzlich zu physischen auch digitale Echtheitsmerkmale (z.B. ein kryptographisch signiertes Zertifikat des Herstellers) integrieren lassen, kann so die Fälschungssicherheit deutlich erhöht werden. Dabei ist jedoch sicherzustellen, dass die enthaltenen Daten in direkter Beziehung zum Inhalt des Dokumentes stehen, damit nicht durch Tausch des RFID-Tags ein anderes Dokument mit einem Echtheitsmerkmal versehen wird.

Seit Herbst 2005 werden in Deutschland maschinenlesbare und mit biometrischen Informationen versehene Reisepässe[143] ausgegeben, um mittelfristig Personen beim Grenzübergang einfacher identifizieren zu können. Auf den RFID-Tags werden die personenbezogenen Daten sowie ein Lichtbild der Inhaber digital signiert gespeichert. Geplant ist, zusätzlich weitere biometrische Daten wie den Fingerabdruck ebenfalls mitzuspeichern. Angekündigt ist ferner die Integration der gleichen Technik auch in Personalausweise. Dies hätte zur Folge, dass nicht nur an Grenzübergängen, sondern generell bei jeder Personenkontrolle die entsprechenden Lesegeräte vorhanden sein müssten. Zur Prüfung der digitalen Signatur benötigen die Lesegeräte eine zumindest vorübergehende Datenverbindung zu einem Zentralrechner. Es ist nicht auszuschließen, dass durch derartige Überprüfungen Bewegungsprofile von Personen entstehen.

Eine Einführung von RFID-Tags in Banknoten z.B. durch die Europäische Zentralbank wird ebenfalls diskutiert, um die Fälschungssicherheit zu erhöhen. Dadurch würde gleichzeitig die Infrastruktur zur detaillierten Erfassung des bisher anonymen Zahlungsverkehrs geschaffen.[144] Mit den bereits vorhandenen Seriennummern lassen sich allerdings auch heute schon Banknoten verfolgen.[145]

Für weitere Dokumente wie Notarverträge oder Briefmarken wird ebenfalls eine digitale Kennzeichnung erwogen. Bei Installation einer bestimmten Software lassen sich Briefmarken der Deutschen Post AG schon heute per Internet kaufen und von einem lokalen Rechner drucken. Dazu müssen die Informationen zur Art der Sendung, Absender und Empfänger an einen zentralen Server übermittelt werden, der Datum, Markenwert, Absender und Empfänger digital signiert in einen 2D-Barcode (genannt Matrixcode) einfügt, der zum Ausdruck an den Besteller übermittelt wird,[146] so dass hier umfangreiche Daten über Kommunikationsbeziehungen anfallen.

---

[143] Für eine technische Beschreibung vergl. Kapitel 7.

[144] MyEuro.info, RFID, http://www.myeuro.info/rfid.php (26.05.2005).

[145] Ibidem, Track your Euro Notes across Europe, http://www.myeuro.info (26.05.2005).

[146] Deutsche Post AG, Wissenswertes zu Stampit, http://www.deutschepost.de/dpag?check=yes&lang=de_DE&xmlFile=1001187 (26.05.2005); Heise Newsticker, Home-Stamping oder Briefmarken selbst gemacht, http://www.heise.de/newsticker/meldung/47178 (26.05.2005).

2.8 Ticketing

Eine eindeutige Identifizierung von Personen ist als Voraussetzung für den Besuch von Großveranstaltungen vorgesehen (Ticketing). So wurden bei der Vergabe der Eintrittskarten für die Fußball-Weltmeisterschaft 2006 seit Anfang 2005 umfangreiche personenbezogene Daten erhoben.[147] Die Karte selbst enthält ein RFID-Tag, auf dem ein Identifikator untergebracht wurde, über den die Daten in einer Datenbank abgerufen und mit dem Personalausweis des Karteninhabers abgeglichen werden können. Eine vergleichbare Anwendung ist bereits in Skigebieten im Einsatz, um ohne größeren Personaleinsatz die Berechtigung für die Nutzung von Skiliften kontaktlos auslesen zu können. Allerdings werden dabei in deutlich geringerem Umfang personenbezogene Daten erfasst und gespeichert als bei den Eintrittskarten für die Fußball-Weltmeisterschaft.

Darüber können mit einem solchen Ticket auch Bezahlfunktionen verbunden werden, die z.B. die schnellere Bezahlung von Getränken oder Snacks in der Halbzeitpause oder in der Skihütte ermöglichen.[148] Die Sicherheit im Stadion wird nicht nur über eine umfassende Videoüberwachung gewährleistet, die über Zoomfunktionen eine gezielte Untersuchung und Überwachung einzelner Stadionbesucher ermöglicht, sondern auch mittels einer Sitzplatzzuweisung über den RFID-Tag auf dem Ticket, wobei dem Inhaber neben seinem Sitzplatz auch die Sektoren im Stadion zugewiesen werden, die er überhaupt betreten darf. Lesegeräte an ausgewählten Punkten sorgen dafür, dass die Bewegungsprofile einzelner Besucher kontrolliert und nachvollzogen werden können.[149] Über den Zugriff auf eine Datenbank mit den Ticketinhabern erschließt sich der Einsatzleitung im Stadium, welcher Besucher welchem Sitzplatz zuzuordnen ist.

Vergleichbare Funktionen einer Bewegungskontrolle verbunden mit einer Zugangs- und Zutrittskontrolle können auch für andere Legitimationskarten wie bspw. die Ausweise von Mitarbeitern[150] genutzt werden. Darüber ist als weitere Anwendung eine Zeiterfassung möglich.

Ein weiteres Beispiel im Bereich des Ticketings ist die Ausgabe von Fahrkarten im Öffentlichen Personen-Nahverkehr (ÖPNV). Eine große Mehrheit der ÖPNV-Betriebe in Deutschland hat sich verpflichtet, Systeme nur noch nach einem Standard auszuschreiben, der die deutschlandweite Nutzung von RFID-basierten Fahrkarten vorsieht. Nach der automatischen Erkennung des Fahrgastes mit Betreten des Transportfahrzeuges erfassen Lesegeräte den Anfangs- und Endpunkt einer Fahrt, die zur Ermittlung und Abrechnung des Fahrpreises an einen zentralen Server übermittelt werden, auf dem als „Nebenprodukt“ aussagekräftige und individuelle Bewegungsprofile der jeweiligen Fahrgäste anfallen.[151]

---

[147] Siehe hierzu: http://www.datenschutzzentrum.de/allgemein/wmticket.htm; http://fifaworldcup.yahoo.com/06/de/030218/1/5r.html; http://www.heise.de/newsticker/meldung/43645 (02.11.2004).

[148] Ibidem.

[149] Siehe hierzu: Bundestagsdrucksache 15/3125 und 15/3190.

[150] Kaiser, 2005.

[151] Vgl. Finkenzeller, op. cit., 2002, 355ff.; Schauer, 2004.

In elektronischer Form kann ein Ticket auch über Mobilfunk erworben werden.[152] Auf seine Bestellung wird dem Kunden über SMS ein 2D-Barcode oder eine eindeutige Zugangsnummer übermittelt, mit der er seine Berechtigung zum Besuch einer Veranstaltung oder zur Inanspruchnahme einer Dienstleistung nachweist. Die Abrechnung erfolgt bargeldlos über den Anbieter des Mobilfunkdienstes.

Die Tags eines solchen Tickets werden im Regelfall auf dem Ticket eingebracht, können aber auch unmittelbar mit der Person des Berechtigten verbunden werden. Eine spanische Diskothekenkette bspw. bietet ein ID-Implantat für den Nachweis einer Zutrittsberechtigung an. Wie auf jeder Chipkarte auch können auf diesem Implantat Personendaten oder Kreditkarteninformationen niedergelegt und ausgelesen werden.[153,154]

2.9 Bildung und Ausbildung

Bisher wird Menschen durch physische Zusammenkunft an Orten wie Schulen, Kindergärten, beruflichen Ausbildungsstätten und Hochschulen Wissen vermittelt. Seit der Einführung des Internets nimmt dieses einen immer breiteren Raum als Medium für die Informationsbeschaffung und -Bereitstellung ein. Neben dem umfangreichen Angebot des World Wide Web lässt sich per E-Mail, über Diskussionsforen oder Konferenz-Systeme (Chat, VoIP, Video-Konferenz) ein Austausch mit Experten oder anderen am gleichen Thema Interessierten über große Entfernungen in kurzer Zeit realisieren.

Suchmaschinen und Online-Enzyklopädien helfen, vorhandene Fachinformationen zu erschließen. Während bei einer herkömmlichen Bibliotheksrecherche es Stunden dauern konnte, eine Quelle zu identifizieren, und durchaus Wochen, bis man diese in Händen hielt, ist dies heute in der Regel ein Vorgang von wenigen Minuten. Da die freie Verfügbarkeit von Informationen ein zentraler Aspekt der Informationsgesellschaft und von „Ubiquitous Learning“ ist, setzt sich im wissenschaftlichen Bereich zunehmend der Ansatz von „Open Access“ durch,[155] was bedeutet, dass neben einer kommerziellen Verwertung wissenschaftlicher Arbeiten in Fachzeitschriften oder Büchern diese ebenfalls frei zugänglich im Internet veröffentlicht werden. Als weiterführender Ansatz erlaubt „Open Content“ z.T. auch die Bearbeitung von Inhalten.[156]

Adaptive Lernsysteme sollen sich anhand von Nutzerprofilen an deren individuelle Lernbedürfnisse anpassen. Gleiche Inhalte werden so verschiedenen Personen mit unterschiedli-

[152] Siehe hierzu http://www.berlinews.de/archiv-2004/3160.shtml ; http://www.handy-parken.de/; http://www.tellus-cities.net/ (05.04.2005).

[153] Neubauer, Harald, Telepolis, http://www.heise.de/tp/deutsch/inhalt/lis/17707/1.html (25.06.2004); Lütge, 2005, S. 30-31.

[154] RFID im Baja Beach Club, http://www.baja-beachclub.com/bajaes/asp/zonavip.aspx (02.11.2004).

[155] Heise Newsticker, Nobelpreisträger für Open Access, http://www.heise.de/newsticker/meldung/50557 (31.08.2004).

[156] Creative Commons Deutschland, http://de.creativecommons.org/ (08.06.2005).

chen Methoden, Geschwindigkeiten und Komplexitäten vermittelt.[157]

2.10 Arbeitswelt

Nicht nur Firmen, die Mitarbeiter im Außendienst beschäftigen, möchten diesen auch unterwegs die Möglichkeit geben, auf Informationsinfrastruktur und Datenbestände der Firma zuzugreifen und Kommunikation mit dem Innendienst, z.B. virtuelle Meetings per Video-Konferenz, einfach, schnell und dabei möglichst vertraulich durchführen zu können.

Auch kleine und mittlere Unternehmen nutzen zunehmend die Chancen einer immer dichteren und leistungsfähigeren Vernetzung. Angesichts einer angespannten Wirtschaftslage bietet sich so im Bereich von Bildschirmarbeitsplätzen z.B. die Möglichkeit, einen neuen Mitarbeiter anstellen zu können, ohne sofort den Kosten für weitere Räumlichkeiten zu begegnen. Der neue Mitarbeiter kann dabei beispielsweise mittels einer per Voice-over-IP arbeitenden Telefonanlage auch gegenüber anrufenden Kunden als normaler Mitarbeiter mit Firmendurchwahl auftreten und seine Tätigkeit mobil oder mit seinem Heimrechner per Internet durchführen.

Im Bereich von digitalen Dienstleistern, z.B. Software-Herstellern, sind bereits Firmen zu finden, die komplett virtuell arbeiten. Die Mitarbeiterinnen und Mitarbeiter arbeiten nicht lokal an einem Ort, sondern kooperieren auf mehrere Standorte verteilt über das Internet bzw. ein Virtual Private Network.

Ubiquitous Computing ist jedoch nicht auf den Bereich intellektueller Dienstleistungen beschränkt. Auch im Handwerk kann z.B. ein Tischler vor Ort beim Kunden mit Werkzeugen, die über entsprechende Sensoren verfügen, Maße komplexer Räumlichkeiten erfassen und an den Betrieb übermitteln, der darauf basierend ein Angebot kalkuliert und die Daten bei Akzeptanz an die Produktionswerkstatt weiterleitet.

Wird in der Pause die Kantine aufgesucht, so lässt sich mit dem Firmenausweis, der auch Zutrittsberechtigung und Arbeitszeiterfassung erlaubt, die gewünschte Mahlzeit bargeldlos bezahlen. Neben den Angaben darüber, wer, wann, wo, wie lange und woran gearbeitet hat, können so auch Informationen über die Ernährung der Angestellten in die Datenbanken des Arbeitsgebers gelangen.

2.11 Reisen, Freizeit und Erholung

Die Nutzung der Möglichkeiten des Ubiquitous Computing erleichtert das Zurechtfinden in fremder Umgebung. Eine vielfältige technische Unterstützung ist bereits heute bei der Routenplanung möglich. Über Internet werden Reiseziele recherchiert, Hotels gebucht, Mietwagen reserviert sowie Tickets für Bahn oder Flugzeug bestellt. Lokalisierungsdienste wie GPS erleichtern es, das Reiseziel zu erreichen. Eine Bündelung unterschiedlicher Dienste zur

[157] Dolog / Wolfgang: Personalisation in Elena – How to Cope with personalisation in distributed eLearning Networks, 2003.

Unterstützung wird z.B. durch einen per Funk vernetzten PDA erreicht.[158] Dieser kann auch das Trägermedium für elektronische Berechtigungen wie Tickets und sonstige Buchungen von der Theaterkarte bis zum Skipass sein, die am gewünschten Ort kontaktlos ausgelesen werden.

Ein solcher PDA unterstützt die Navigation zum Reiseziel und vor Ort unter Berücksichtigung individueller Präferenzen.[159] Er kann Informationen über aktuelle Veränderungen vom Stau auf der Autobahn, den Flugplänen bis zur Unwetterwarnung empfangen und auswerten sowie über aktuelle Veranstaltungen und wichtige Ereignisse informieren. Zur Prozessbeschleunigung kann er den Dienstleistern vom Reiseunternehmen bis zum Hotel die zur Anmeldung erforderlichen Daten zur Verfügung stellen. Auf diesem PDA kann der Reisende seine individuellen Umgebungspräferenzen mitführen (z.B. Klimaanlage, Fernsehprogramm, Erreichbarkeitseinstellungen, Telefonbuch etc.), die bspw. nach Freigabe vom Hotelzimmer ausgelesen werden. In fremdsprachiger Umgebung kann der PDA als Übersetzungshilfe dienen, indem er über Sensoren die jeweiligen Texte auf Hinweisschildern, Fahrplänen etc. ausliest und in der gewünschten Sprache ausgibt.

Durch Ubiquitous Computing ergeben sich auch im Unterhaltungsbereich, insbesondere bei Computer-unterstützten Spielen („Gaming“), neue Perspektiven.[160] Neue Human-Computer-Interfaces sowie Location-based Services erweitern Spielkonzepte mit dem Mobiltelefon, Spielkonsolen oder Online-Games.[161] Beispiele für ein Ubiquitous oder „Pervasive Gaming“[162] [163] sind multimediale Live-Rollenspiele (LARP), in denen die Computerunterstützung die Einhaltung der Spielregeln ermöglichen soll.

2.12 Militärische Anwendungen

Auch für militärische Zwecke sind Anwendungen einer RFID-basierten Logistik anzutreffen, um die Zulieferung und Verwendung von Produkten und Objekten zu verwalten und zu steuern. Daneben gibt es aber auch eine Reihe weiterer militärspezifischer Einsatzgebiete, die auch einen Ausblick auf zukünftige zivile Anwendungen erlauben. Aufgrund der branchenüblichen Geheimhaltung ist davon auszugehen, dass neben den bekannten Techniken weitere in Erprobung und im Einsatz sind, über die auf den öffentlich zugänglichen wissenschaftlichen Informationskanälen noch nichts zu erfahren ist. Die Effizienz dieser Techniken ist von vitalem Interesse für ihre hauptsächlich staatlichen Nutzer, so dass von einer stetigen Wei-

[158] Vgl. IST Advisory Group, 2001, 4, 26ff.

[159] Coroama et al. 2003, S. 83f.

[160] Björk et al., Personal and Ubiquitous Computing - Special Issue on Ubiquitous Gaming, 6, 2002, S. 358–361.

[161] Vgl. Forrester Report ‘‘Pervasive Gaming Goes Mainstream’’, August 2000, zitiert bei: Björk et al., 2002.

[162] Für Vorformen siehe z.B. Fabien Girardin, Pervasive Game Development Today, 2005, http://www.girardin.org/fabien/catchbob/pervasive/ (26.05.2005).

[163] IPerG - Projektsammlung zu Pervasive Games, http://www.pervasive-gaming.org (26.05.2005).

terentwicklung ausgegangen werden kann.

Entsprechendes gilt für die erforderlichen Gegenmaßnahmen, um feindlichen oder feindlich übernommenen UC-Systemen nicht ausgeliefert zu sein. Da es auch sehr kritische Haltungen zu Ubiquitous Computing gibt, ist mit dem Auftauchen von Gegenmaßnahmen auch im zivilen Bereich zu rechnen.[164]

Die Ausrüstung insbesondere von Soldaten hat sich in den letzten Jahren um Komponenten des Ubiquitous Computing erweitert. Es ist zu erwarten, dass sich dieser Trend in den nächsten Jahren noch fortsetzen wird. Waren Helmvisier-Displays, die die Sicht des Trägers um taktische Informationen erweitern, in der Vergangenheit vornehmlich noch Piloten vorbehalten, gibt es inzwischen Prototypen auch für Infanteristen, die z.B. eine Stadt einnehmen und sichern sollen. Neben Angaben zur eigenen Position können auf diese Weise von Satelliten oder Aufklärungseinheiten als potentielle Gefahr erkannte Bereiche markiert und den zuständigen Einheiten bereitgestellt werden. Die Systeme erlauben zugleich eine ständige Kommunikation mit einem Befehlsstand, der so aktuelle Informationen erhält, auswertet und entsprechende Anweisungen erteilen kann.

Militärische Einheiten sind darauf angewiesen, Informationen über ihre Umgebung z.B. über spezielle Sensoren zu erfassen und auszuwerten, um sich auf diese Weise einen taktischen Vorteil zu verschaffen. Dabei müssen die Sensoren möglichst passiv arbeiten, damit ausgeschlossen werden kann, dass Dritte die betreffende Einheit über Sensor-Emissionen erkennen und ausschalten können. So werten bspw. U-Boote Geräusche in Echtzeit aus und gleichen diese mit Datenbanken ab, um im Falle eines festgestellten nicht-natürlichen Ursprungs auf feindliche Aktivitäten frühzeitig reagieren zu können.

Für die Überwachung größerer Bereiche und die Erkennung von feindlichen Aktivitäten kann Smart Dust[165] zur Anwendung kommen. Mit entsprechenden Sensoren versehen kann Smart Dust z.B. Schwingungen des Bodens registrieren und an ein Auswertungssystem übermitteln, das sie als spezifische Muster bestimmten feindlichen Einheiten, z.B. bestimmten Fahrzeugtypen, zuordnen kann.

[164] Ein erster Ansatz sind der Tag-Finder von eMedia, http://www.emedia.de/@897V3XTVrhFM/bin/hw.pl?Aktion=P&Proj_Nr=0502_1 (08.06.2005), mit dem RFID-Tags aufgefunden werden können, sowie der RFID-Scanner-Detektor-Armreif des FoeBuD, https://shop.foebud.org/product_info.php/products_id/76 (08.06.2005), der die EM-Felder von Lesegeräten meldet.

[165] Thoms, Henrik: Smart Dust, Weimar, 2003, http://www.uni-weimar.de/~heymann/Public/manet_maus.pdf (26.05.2005).

2.13 Literatur

Bager, Jo / Violka, Karsten: Das denkende Haus bauen, c't - Magazin für Computertechnik, 17, 2001, S. 114ff.

Bittner, Jochen: Denn sie wissen, was wir tun – Geheimdienste und Polizei erfahren mehr über die Bevölkerung als die Verfassung erlaubt, Die Zeit, 03.03.2004, S. 3.

Björk, Holopainen et al.: Personal and Ubiquitous Computing – Special Issue on Ubiquitous Gaming, 6, 2002, S. 358–361.

Bohn, Jürgen / Coroama, Vlad / Langheinrich, Marc, et al.: Allgegenwart und Verschwinden des Computers – Leben in einer Welt smarter Alltagsdinge. In: Grötker, Ralf (Hg.): Privat! Kontrollierte Freiheit in einer vernetzten Welt, 2003, S. 195-245.

Bundesamt für Sicherheit in der Informationstechnik (BSI). Integrierte Gebäudesysteme - Technologien, Sicherheit und Märkte, 2002.

Coroama, Vlad / Hähner, Jörg / Handy, Matthias, et al.: Leben in einer smarten Umgebung: Ubiquitous-Computing-Szenarien und -Auswirkungen, 2003, http://www.vs.inf.ethz.ch/publ/papers/szenarien-FINAL.pdf (26.10.2004).

Davies, Nigel / Gellersen, Hans-Werner: Beyond Prototypes: Challenges in Deploying Ubiquitious Systems, Pervasive Computing Magazine, 1, 1, 2002, S. 26-35.

Dolog, Peter / Wolfgang, Nejdl: Personalisation in Elena – How to Cope with personalisation in distributed eLearning Networks, 2003, http://www.l3s.de/~dolog/pub/sinn2003.pdf (29.06.2005).

Doukidis, Georgios / Pramatari, Katerina: Supply Chains of the future and Emerging Consumer-Based Electronic Services, Spinger LNCS 3746, 2005, S. 571-581.

Finkenzeller, Klaus: RFID-Handbuch, 2002.

Gershenfeld, Neil: Wenn die Dinge denken lernen –Zukunftstechnologien im Alltag, Econ Verlag, 2000.

Heise Online: WM-Tickets vs. Datenschutz 0:1, Heise Verlag, http://www.heise.de/newsticker/meldung/55419 (21.01.1005).

Helal, Sumi / Mann, William / El-Zabadani, Hicham, et al: The Gator Tech Smart House – A Programmable Pervasive Space, IEEE Computer Magazine, 3 (38), 2005, S. 50-60, http://csdl.computer.org/dl/mags/co/2005/03/r3050.pdf (06.05.2005).

Hellweg, Eric: RFID zwischen Hype und realen Anwendungen, Technology Review 2004, http://www.heise.de/tr/aktuell/meldung/49197 (11.02.2004).

IST Advisory Group: Scenarios for Ambient Intelligence in 2010, published in 2001, http://www.hltcentral.org/usr_docs/ISTAG-Final.pdf (02.03.2005).

Kaiser, Tobias: Fürs Leben markiert, Die Zeit, 2005, S. 30.

Kandl, Dunja: Sturm auf die Bastille, RFID-Forum 2004, 01, S. 12-15.

Kern, C. / Wendl, G.: Tierkennzeichnung - Einsatz elektronischer Kennzeichnungssysteme in der intensiven und extensiven Rinderhaltung am Beispiel Deutschland und Australien, Landwirtschaft 3, 1997, S. 156-157.

Kuri, Jürgen: Das persönliche Haus, c't - Magazin für Computertechnik, 22, 1999, S. 194.

Langheinrich, Marc: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte für RFID Technologie, 2003, http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf (09.08.2004).

Li, Dong / Kehoe, Dennis / Drake, Paul: Dynamic planning with a wireless product identification technology in food supply chains. International Journal of Advanced Manufacturing Technology, Springer 2005.

Liu, Michael R. / Zhang, Q. L. / Ni, Lionel M. / Tseng, Mitchell M.: An RFID-Based Distributed Control System for Mass Customization Manufacturing, LNCS 3358, S. 1039-1049, Springer 2004.

Luckett, D.: The supply chain, BT Technology Journal, Vol. 22, No. 3, 2004, S. 50-55.

Lütge, Gunhild: Der Allesscanner, Die Zeit, 2005, S. 30-31.

Mattern, Friedmann: Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Mattern, Friedmann (Hg.), Total vernetzt, 2003, S. 1-41.

Ostler, Ulrike: RFID: Die Revolution lässt sich noch etwas Zeit, Silicon.de ~ Das Info-Netzwerk für IT und Business, 2003, http://www.silicon.de/cpo/hgr-mobile/detail.php?nr=10252) (19.10.2004).

Posch, Karl-Heinz / Epple, Roland: Hier ist Kombinationsgabe gefragt, RFID-Forum, 7/8, 2004, S. 16-20.

Schauer, Andreas: Volle Fahrt voraus, RFID-Forum, 5, 2004, S. 24-28.

Silicon.de: Philips setzt RFID gegen Vogelgrippe und BSE, Silicon.de ~ Das Info-Netzwerk für IT und Business, 18.02.2004, http://www.silicon.de/cpo/news-mobile/detail.php?nr=13249 (27.10.2004).

Stajano, Frank: Security for Ubiquitous Computing, Chichester (UK), John Wiley & Sons, 2002.

Vrba, Pavel / Macurek, Filip / Marík, Vladimír: Using Radio Frequency Identification in Agent-Based Manufacturing Control Systems, Springer LNAI 3593, 2005, S. 176-178.

3 Bestimmungsfaktoren des Ubiquitous Computing

3.1 Technische Bestimmungsfaktoren des Ubiquitous Computing

Benjamin Fabian

3.1.1 Einleitung

Die Bestimmung der wesentlichen technischen Faktoren[166], die die Entwicklung des Ubiquitous Computing[167] beeinflussen können, ist aufgrund des hohen Grades an Interdisziplinarität in diesem Forschungsgebiet nicht einfach. Einerseits bestehen zahlreiche Wechselwirkungen der Technik mit psychologischen, sozialen und ökonomischen Bestimmungsfaktoren, andererseits entwickelt sich ein Phänomen wie Ubiquitous Computing dynamisch und iterativ. Unter diesen Bedingungen können reale oder auch nur antizipierte Wirkungen eines Teilprozesses, Entwicklungsstadiums oder Anwendungsbereichs die weitere technische Entwicklung beeinflussen und damit zu Bestimmungsfaktoren der nächsten Stadien werden.

Im Folgenden werden die wesentlichen Einflussfaktoren der technischen Entwicklung aufgezeigt, die für eine Vielzahl der Anwendungen mit hoher Wahrscheinlichkeit von Bedeutung sein werden. Sie dienen als Variablen für Szenarien, die verschiedene zukünftige Entwicklungsvarianten des Ubiquitous Computing und ihre Auswirkungen auf die informationelle Selbstbestimmung beschreiben.

3.1.2 Miniaturisierung

„But where does Moore's Law come from? What is behind this remarkably predictable phenomenon? ... In my view, it is one manifestation (among many) of the exponential growth of the evolutionary process that is technology."

Kurzweil (2001)

Die Vision des „Internets der Dinge"[168], immer leistungsfähigere und vernetzbare Computer in immer mehr Objekte der physischen Welt zu integrieren, beruht auf der Miniaturisierung der eingesetzten technischen Komponenten als fundamentaler Vorbedingung. Zunehmende Miniaturisierbarkeit von Chips hat somit einen stark fördernden Einfluss auf die Entwicklung

[166] Unsere Induktion von den konkreten technischen Entwicklungen zu den abstrakten Bestimmungsfaktoren basiert auf den TAUCIS-Kapiteln Technische Grundlagen (Kap. 1) und Anwendungsfelder (Kap. 2). Vergleichbare Ansätze zur Klassifizierung von Einzeltechnologien bei Klaas, 2003; Fleisch/ITU, 2005, S. 11ff.; Mattern, 2005.

[167] Im allgemeinen Sinne von Weiser (1991, 1993), mit Lyytinen (2002) als Obermenge von Mobile und Pervasive Computing aufgefaßt, hier auch inklusive Ambient Intelligence (ISTAG 2003).

[168] Keineswegs nur auf RFID beschränkt, wo sich technische Hürden aber schon heute klar zeigen. Zum Zusammenhang Ubiquitous Computing und Internet der Dinge: Mattern, 2003, S. 2.

des Ubiquitous Computing, eventuelle Grenzen einer Miniaturisierung dagegen könnten seine Entwicklung hemmen, falls die benötigten Komponenten noch zu groß sind, um in für ein Anwendungsfeld wichtige kleine Gegenstände eingebaut zu werden.

Einen optimistischen Hinweis auf die weitere Entwicklung bietet Moore's Law[169], die bekannte heuristische Faustregel, die bereits seit vielen Jahren die Entwicklung der Leistungsfähigkeit von Computerchips mit gutem Erfolg beschreibt. Nach Moore's Law, ursprünglich 1965 aufgestellt, verdoppelt sich die Integrationsdichte integrierter Schaltkreise, d.h. die Anzahl von Transistoren pro Flächeneinheit, etwa alle ein bis zwei Jahre. Daraus folgt, dass bei gleich bleibender Leistung kleinere Bauformen möglich werden. Diese Beobachtung wurde mit einigem Erfolg verallgemeinert und auf andere Bereiche der Computertechnik übertragen, visionär und noch allgemeiner gefasst als ein „Law of Accelerating Returns".[170]

Moore's Law ist im Wesentlichen bis heute gültig und wird wahrscheinlich auch in der näheren Zukunft Bestand haben.[171] Einen sehr wichtigen Beitrag zur weiteren Miniaturisierung wird zukünftig die Nanotechnologie leisten.[172] Neben der Forschung zu eigentlichen Nanomaschinen wird auch deren optische Kommunikation große Bedeutung erlangen. Bei langfristiger Betrachtung ist daher eine für die Mehrzahl denkbarer Anwendungen ausreichende Miniaturisierbarkeit von Komponenten und somit eine fördernde Wirkung auf die Entwicklung des Ubiquitous Computing sehr wahrscheinlich.[173]

Es ergibt sich allerdings als mögliches Hemmnis das Problem, wie diese kleinen, in Gegenstände integrierten Geräte durch Updates auf einem aktuellen technischen Stand von Hard- und Software gehalten werden können. Auch kann es notwendig sein, einzelne Hardware-Komponenten wegen eines Funktionsausfalls auszutauschen. Relativ unproblematisch erscheint dies lediglich in Billigprodukten mit einer relativ kurzen Lebensdauer, jedenfalls unter der Voraussetzung, dass das neue Bauteil bzw. die Software mit den übrigen Komponenten des ubiquitären Umfeldes interoperabel ist. Sobald die Bauteile eines Ubiquitären Computing in langlebige Objekte eingebettet sind oder als Bestandteil von Baumaterialien nicht mehr ohne Weiteres aus ihrer Umgebung zu isolieren sind, bedarf das Update-Problem einer unter den Gesichtspunkten der Gebrauchstauglichkeit und der Wirtschaftlichkeit zufriedenstellenden Lösung. Dies kann viele Anwendungen des Ubiquitous Computing betreffen, besonders aber Entwürfe einer „Ambient Intelligence" wie bspw. das so genannte Smart Home.[174]

Die Fähigkeit zu Updates und damit insbesondere zur Fehlerbehebung wird bei einer zunehmenden Vernetzung insbesondere einen wichtigen Einfluss auf die Sicherheit des jewei-

---

[169] Intel Research zu Moore's Law, http://www.intel.com/research/silicon/mooreslaw.htm (20.06.2005); Mattern, 2005, S. 4ff.

[170] Kurzweil, 2001.

[171] Diskussion z.B. bei Wikipedia: Wikipedia zu Moore's Law: http://en.wikipedia.org/wiki/Moore%27s_law (27.06.2005).

[172] BMBF zur Nanotechnologie: http://www.bmbf.de/de/nanotechnologie.php (20.06.2005).

[173] Allerdings siehe zu möglichen Risiken speziell der Nanotechnik: Lauterwasser, 2005.

[174] Beispieldesign für ein Smart Home: The Gator Tech Smart House, Helal et al., 2005.

ligen Systems bekommen (s.a. unten Kap. 3.1.8). Gelingt mit anderen Worten die Lösung des Update-Problems nicht, dann werden die jeweiligen Anwendungssysteme nicht oder nicht rechtzeitig an das erforderliche Sicherheitsniveau angepasst werden können. Sicherheitslücken beschränken jedoch in aller Regel auch die Funktionalität der Anwendungen. Mit dem Grad der Vernetzung steigt die Abhängigkeit des Gesamtsystems von einzelnen Komponenten, so dass der Ausfall bzw. die Störung einzelner Bauteile die Funktionalität des Gesamtsystems beeinträchtigen wird. Im Ergebnis wird eine unzureichende Lösung des Update-Problems die Funktionalität der Anwendungen beeinträchtigen und damit die Entwicklung des Ubiquitären Computing behindern.

Eine weitere Einflussgröße im Zusammenhang mit der Miniaturisierung ist die unter dem Gesichtspunkt des Umweltschutzes relevante Frage, ob und auf welche Weise die Chips beim Recycling vom Trägerobjekt getrennt werden können.[175] Je enger die Chips und Sensoren mit ihren Trägerobjekten verwoben sind, desto aufwändiger wird im Rahmen des Recyclings die Trennung. Lassen sie sich aber nicht oder nur aufwändig trennen (z.B. bei Smart Materials, iSeeds[176], Trägermedien wie Baumaterialien, Tapeten, Farbe), steigen die Entsorgungskosten, weil die Trägerobjekte mit integrierten Chips und / oder Sensoren tendenziell als Elektroschrott zu bewerten sein werden.

Modularisierung, Austauschbarkeit der Hardwarekomponenten und möglichst weit reichende Fähigkeit zu Software-Updates werden zu wichtigen Unterfaktoren der weiteren Entwicklung bei fortschreitender Miniaturisierung. Eine Lösung dieser Probleme erscheint wahrscheinlich, die Hemmwirkung auf die Entwicklung des Ubiquitous Computing wird unserer Einschätzung nach nicht entscheidend sein, sie kann allerdings andere Faktoren wie Sicherheit graduell beeinflussen.

3.1.3 Energieversorgung

„Energy is only one of many resources needed for mobile computing. ... But their scarcity does not have the grim finality of a dead battery."

Satyanarayanan (2005, S. 2).

Ein weiterer wichtiger Bestimmungsfaktor für die weitere technische Entwicklung ist die Lösung der Energieversorgung für die Anwendungen des Ubiquitären Computing. Wie versorgt man zahllose eingebettete, sowohl stationäre als auch mobile Geräte dauerhaft mit Energie? Plakativ formuliert: Wie funktioniert der Batteriewechsel im Ubiquitous Computing? Aus dieser Fragestellung ergeben sich zwei Teilaspekte, nämlich die Energiesparsamkeit sowie neue Formen der Energieversorgung.

Mit der Miniaturisierung und der Vielzahl der Objekte wächst die Bedeutung, energiesparende Hardware und Software zu entwickeln. So ist zum Beispiel bei Sensornetzen der Ener-

[175] Grundlegend hierzu die Studie von Hilty et al., 2005.

[176] McCloskey, 2004, S. 28ff.

gieverbrauch ein wichtiger Faktor für ihre maximale Reichweite sowie die Häufigkeit und Dauer ihrer Kommunikationsfähigkeit. Der Energieverbrauch muss bspw. bereits systemseitig bei der Entwicklung von Routing-Protokollen berücksichtigt werden. Der Energieverbrauch beeinflusst aber nicht nur die Funktionalität der Anwendungen, sondern auch ihre Sicherheit. In der Gegenwart zeigt sich, dass geringe Rechenleistung von Kleinstgeräten den Einsatz starker Kryptographie und damit starker Sicherheitsfeatures verhindern kann. Entsprechendes gilt wahrscheinlich auch noch in Zukunft für den Energieverbrauch, der sowohl die Kommunikationsfähigkeit im Ubiquitären Computing beschränkt als auch die Verwendung kryptographischer Sicherheitsfeatures.[177] Ganz allgemein erleichtert ein niedriger Energieverbrauch als Kostenfaktor den Einsatz einer Vielzahl von Geräten im für Ubiquitous Computing benötigten Maßstab.

Vor diesem Hintergrund wird die Gewinnung von Energie aus der Umgebung, so genanntes „Ernten von Energie“ (Energy Harvesting)[178] u.a. aus Bewegung, Temperaturwechsel oder Schall, entscheidende Bedeutung für die Entwicklung zukünftiger Anwendungen des Ubiquitären Computing erlangen. Auch könnten wasserstoffbasierte oder mikrobielle Brennstoffzellen[179] die Energieversorgung langfristig erleichtern. Der Wirkungsgrad solcher Verfahren und ihre Anwendbarkeit für Ubiquitous Computing lassen sich zur Zeit noch nicht abschließend beurteilen.

Entsprechendes gilt für die Bemühungen, Techniken zur drahtlosen Energieübertragung, wie zum Beispiel über Funk (passive RFID-Chips) oder Laser, zu entwickeln. Hier stellen sich Fragen zur Effizienz, Reichweite, Topologie (hemmende Materialien, eventuelle Notwendigkeit einer Sichtlinie) und der Skalierbarkeit solcher Ansätze für größere Netzstrukturen.

Eine hemmende Wirkung für die Entwicklung des Ubiquitären Computing wirft der Energieverbrauch schließlich auch unter dem Gesichtspunkt des Umweltschutzes bzw. Klimaschutzes auf, insbesondere wenn dieser Verbrauch mit der Vielzahl der eingesetzten Geräte und Anwendungen stark ansteigt. Entsprechendes gilt auch für die Energiekosten, die bei ohnehin steigenden Energiepreisen die privaten und gewerblichen Haushalte bereits heute belasten und die Bereitschaft für weitere Aufwendungen beschränken.

Die Frage der Energieversorgung ist mit anderen Worten noch nicht abschließend gelöst. Sie kann sich als durchaus starkes Hindernis für die zukünftige Entwicklung des Ubiquitären Computing erweisen.

3.1.4 Interoperabilität

„The danger is that proprietary systems become the only option for users and that market dominance by non-European companies in fields such as operating systems expands further

[177] Stajano, 2002, S. 138ff.

[178] Satyanarayanan, 2005.

[179] Wikipedia, s.v.: http://de.wikipedia.org/wiki/Brennstoffzelle (21.06.2005).

to emerging fields. This would not only limit innovation: it would jeopardise the vary concept of 'seamlessness' in the AmI environment, and weaken the position of European industry."

IST Advisory Group (2003, S. 20).

Von entscheidender Bedeutung für die Entwicklung des Ubiquitären Computing und seiner Anwendungen wird die Interoperabilität der einzelnen Geräte, Programme und Dienste sein. Die Leitfrage lautet: Wie stellt man die flexible Interaktion von Geräten, Softwareagenten und Diensten im Ubiquitous Computing sicher? Die Vielzahl an Komponenten und ihre (teilweise) Mobilität verdeutlichen die Notwendigkeit einer möglichst hohen Interoperabilität.[180]

Unter Interoperabilität ist die „Fähigkeit unabhängiger, heterogener Systeme" zu verstehen, „möglichst nahtlos zusammen zu arbeiten, um Informationen auf effiziente und verwertbare Art und Weise auszutauschen bzw. dem Benutzer zur Verfügung zu stellen, ohne dass dazu gesonderte Absprachen zwischen den Systemen notwendig sind."[181]

Aus technischer Sicht sind Normen und offene Standards besonders bei Kommunikation und Datenformaten zentrale Voraussetzungen für die Interoperabilität.[182] Bedeutsame Beispiele sind XML als universelles Datenformat sowie eine mögliche allgemeine Konvergenz zum Internet-Protokoll (IPv4 / IPv6) als Vermittlungsschicht der Kommunikation. Aber auch kompatible Schnittstellen für (Web)-Services sowie gegenseitig übersetzbare Bedeutungsmodelle für semantisches Web und Software-Agenten werden für Anwendungen des Ubiquitous Computing von erheblicher Bedeutung sein.

Hohe Interoperabilität von möglichst vielen Systemen bildet aus technischer Sicht einen stark fördernden Faktor für Ubiquitous Computing. Dem können ökonomische Gesichtspunkte wie z.B. eine zunehmende Patentierung, die Bildung und Verteidigung von Monopolsstellungen oder die Bündelung von Inhalten (Content) mit proprietärer Technik entgegenstehen. Die Entwicklung der Internetstandards, die Vitalität der Open Source-Bewegung und die allgemein förderliche Wirkung von Normen[183] geben Anlass für einen vorsichtigen Optimismus.

Ein anderer möglicherweise hemmender Aspekt ist die Auswirkung der Interoperabilität auf die Sicherheit von Systemen: Es ist nicht von vornherein klar, ob der Sicherheitsgewinn durch die Offenheit von Schnittstellen und eventuell ganzen Systemen (Transparenz, „no obscurity") einen eventuellen Sicherheitsverlust aufgrund einer erhöhten Angreifbarkeit (mehr Schnittstellen zu anderen Systemen) wettmacht. Diese Frage wird letztlich nur auf der Ebene von konkreten Anwendungen verlässlich beurteilt werden können.

Interoperabilität kann eine hemmende Wirkung für die Entwicklung des Ubiquitären Computing zukommen, wenn sie den Datenaustausch zwischen den Systemen erleichtert und auf diese Weise die informationelle Selbstbestimmung der Nutzer beeinträchtigt. Auch hierzu

---

[180] Zu den Anforderungen an Software siehe u.a. Tandler, 2001, S. 97.

[181] Wikipedia, s.v.: http://de.wikipedia.org/wiki/Interoperabilität (21.06.2005); Siehe auch: http://www.interoperabilität.de/ (21.06.2005).

[182] Für Ubiquitous Computing siehe z.B. Davies, 2002, S. 32; Helal, 2005.

[183] Siehe z.B. Swann, 2000.

müssen konkrete Systeme und ihre speziellen Datenflüsse betrachtet werden. Der Zusammenhang der Bestimmungsfaktoren der sozialen Akzeptanz sowie des normativen Datenschutzes wird weiter unten dargestellt (Kap. 3.2, 3.4)

3.1.5 Vernetzung

"In fact, even Internet experts admit having more and more troubles getting (and keeping) their arms around the essential components of this largescale, highly-engineered network that has all the features typically associated with complex systems – too complicated and hence ill-understood at the system-level, but with often deep knowledge about many of its individual components; resilient to designed-for uncertainties in the environment or individual components ("robustness"), yet full of surprising behavior ("emergence"), including a natural tendency for infrequently occurring, yet catastrophic events ("fragility")."

Willinger (2002, S. 2)

Neben der Miniaturisierung stellt die Vernetzung von Objekten einen wichtigen und oft diskutierten Aspekt des Ubiquitous Computing dar. Die Vernetzung ist zwar ihrerseits abhängig von den Bestimmungsfaktoren Energieversorgung und Interoperabilität, wird hier aber aufgrund ihres starken Einflusses und ihrer Wechselwirkungen mit ökonomischen und sozialen Aspekten einzeln aufgeführt.

Diese Wechselwirkungen manifestieren sich besonders in der Existenz einer Vielzahl von heuristischen Faustregeln, die einen Zusammenhang zwischen dem „Wert" eines Netzes und der Anzahl seiner Teilnehmer herzustellen versuchen. Beispiele[184] sind Sarnoff's Law[185], Metcalf's Law[186] und Reed's Law[187]. Obwohl die letzten beiden sich in der Praxis als viel zu optimistisch erwiesen haben[188], zeigen sie doch die hohe soziale und ökonomische Bedeutung von Vernetzung und der dadurch erleichterten Bildung von Gruppen mit ähnlichen Interessen.

Allgemein besteht die Frage, ob grundlegende Designentscheidungen hinsichtlich der Architektur des Internets[189] langfristig auch für Ubiquitous Computing beibehalten werden. So sehen einige Autoren zum Beispiel das End-to-end-Prinzip[190] durch ökonomische Faktoren[191] – u.a. die Kontrolle über den Zugang zum Netz – oder Zensurbestrebungen bedroht,

---

[184] Rheingold, 2002, S. 56ff.

[185] Broadcast (unidirektional): W(n) = c*n, W Wert, n Anzahl Teilnehmer, c konstant.

[186] $W(n) = c*(n^2 - n)$, quadratischer Zuwachs (mögliche Verbindungen).

[187] $W(n) = c*(2^n - n - 1)$, exponentieller Zuwachs; betont sozialen Wert von Gruppenbildung.

[188] Siehe Odlyzko, 2005, der als alternative Faustregel W(n) = c*n*log (n) begründet.

[189] Eine Übersicht zum Design und Diskussion bieten Willinger, 2002; Bush (RFC 3439), 2002.

[190] Einfachheit im Kommunikationsnetz selbst, möglichst viele Funktionen in den Endpunkten, Saltzer, 1984.

[191] Lemley, 2001; Lessig, 2002, bes. S. 34ff.

die Filterfunktionen auf der Anwendungsschicht[192] in Routern verwenden.

Aus technischer Sicht bietet sich IPv6 als Netzwerkprotokoll im Ubiquitous Computing an. Neben dem gewaltigen Adressraum und der Möglichkeit zur Autokonfiguration steht mit Mobile-IPv6 eine möglicherweise sehr bedeutende Technik für mobile Geräte zur Verfügung. IPv6 stellt allerdings zur Zeit noch eine disruptive Technologie[193] im Gegensatz zum allgemein verbreiteten IPv4 dar; d.h. man kann seine Durchsetzung zunächst in Nischenmärkten erwarten, da sein Mehrwert gegenüber IPv4 im klassischen Internet noch zu gering ist. In einem „Internet der Dinge" des Ubiquitous Computing könnte sich IPv6 aufgrund seines zur Verfügung stehenden Adressraumes einen eigenen Markt erschließen. Hierfür ist das Erreichen einer „kritischen Masse"[194] entscheidend, ab der seine Entwicklung durch Netzwerkeffekte zum Selbstläufer wird. Es ist möglich, dass sich diese kritische Masse zunächst in den Märkten Asiens bilden wird.[195] Indikatoren für diese These sind neben der Bedeutung Japans[196] und Chinas im Markt der mobilen Geräte auch der knappe Anteil dieser Länder an zugeteilten IPv4-Adressen.[197]

Unabhängig von der konkreten Art der verwendeten Vermittlungsschicht gilt, dass Anwendungen des Ubiquitären Computing allgemein stark abhängig sind von der Möglichkeit, Objekte aus der Ferne zu adressieren und anzusprechen. Unter dieser Voraussetzung ist die Fähigkeit zur Vernetzung ein zentraler Bestimmungsfaktor für die zukünftige Entwicklung des Ubiquitous Computing.

3.1.6 Human-Computer Interfaces

„Humans speak, gesture, and use writing utensils to communicate with other humans and alter physical artifacts. These natural actions can and should be used as explicit or implicit input to ubicomp systems."

Abowd (2000, S. 32)

Entscheidend für die Akzeptanz von zukünftigen ubiquitären Systemen wird das Design der Mensch-Maschinen-Schnittstellen sein. Dabei wird die gewaltige Anzahl von Systemen, mit denen ein einzelner Mensch in Zukunft interagieren muss, eine bedeutende Rolle spielen. Es steht zu erwarten, dass die Bereitschaft der Menschen, sich auf solche Schnittstellen einzulassen, unter dem Gesichtspunkt sozialer Akzeptanz im Sinne einer natürlichen Abwehrhal-

[192] Cherry, 2005.

[193] Im Sinne von Christensen, 2003; IPv6 derart klassifiziert z.B. von Loshin, 2004.

[194] Nach Rogers, 2003, S. 343 ff.; der Grad an Verbreitung „after which further diffusion becomes self-sustaining" (S. 343).

[195] Allerdings sollen auch alle US-Bundesbehörden bereits bis 2008 ihre Netze auf IPv6 umstellen, vergl. Heise Newsticker, 30.06.2005, http://www.heise.de/newsticker/meldung/61250 (30.06.2005).

[196] Siehe z.B. Rheingold, 2002, S. 1ff.

[197] Loshin, 2004, S. 17.

tung der Entwicklung des Ubiquitous Computing zunächst hemmend entgegenstehen wird. Maßgebend wird letztlich sein, ob die Anwendungen einen überzeugenden Nutzen haben und wie schnell ihre Verbreitung vonstatten gehen wird.

Zentrales Designparadigma ist das so genannte Human-centered Computing[198], das den Fokus von der bloßen Adaption des Menschen an die Maschine zu einer zentralen Stellung des Menschen verschiebt, der mit seinen Anforderungen an eine einfach nutzbare Technik deren Gestaltung bestimmt.[199]

Erforderlich sind neuartige Interfaces[200], die dieses Paradigma einerseits berücksichtigen, aber auch eine Schnittstelle zu vielen Geräten gleichzeitig bilden können. Hierzu müssen Strategien zur Filterung von Informationen entwickelt werden, die die Ökonomie der Aufmerksamkeit (Attention Economy)[201] seitens der Nutzer berücksichtigen. Andernfalls wird sich der Wettbewerb um die knappe Ressource Aufmerksamkeit im Ubiquitous Computing zuspitzen.

Auf der anderen Seite wird es immer mehr Systeme ohne eigene Interfaces zum Menschen und zunehmende Maschine-zu-Maschine-Interaktion[202] geben, deren Kontrolle aufgrund mangelnder Transparenz schwierig wird.[203] Eine zunehmende Verselbständigung und Undurchschaubarkeit technischer Prozesse könnten als bedrohlicher Kontrollverlust empfunden werden und hemmend auf die Entwicklung des Ubiquitous Computing wirken.[204] Begrenzte Aufmerksamkeit und Wunsch nach Kontrolle werden zu zentralen Gegenpolen im Interfacedesign.

3.1.7 Kontextverständnis

"The most potentially interesting, challenging, and profound change implied by the ubiquitous computing era is a focus on calm. If computers are everywhere they better stay out of the way, and that means designing them so that the people being shared by the computers remain serene and in control. Calmness is a new challenge that UC brings to computing."

Weiser (1996)

Um „Calm Computing" im Sinne von Weiser[205] erreichen zu können, müssen viele Aufgaben an die umgebende Technik delegiert werden. Wichtig werden zum Beispiel Softwareagenten, die alltägliche Aufgaben wie zum Beispiel das Aushandeln von Parametern in adaptiven

[198] Zum Begriff Dertouzos, 2001; Mattern, 2003, S. 4.

[199] Grundlegend dazu: Shneiderman, 2004; Raskin 2000; Norman, 1999.

[200] Gute Übersicht über neue Interfaces bieten Stajano, 2002; Lipp, 2004.

[201] Prägend Davenport, 2001.

[202] Gow/ITU, 2005, S. 18.

[203] Siehe auch unten zu den rechtlichen Bestimmungsfaktoren: Roßnagel/Müller, 2004.

[204] Abowd 2002, S. 51.

[205] Weiser, 1996.

Umgebungen übernehmen können. Entscheidend hierfür ist es, den Kontext[206] des Nutzers (z.B. Ort, Verhalten, Verfassung und Vorlieben) treffend zu modellieren, damit die Technik flexibel und sinnvoll, in diesem Sinne also „intelligent" reagieren kann.

Somit gibt es, neben der absichtlich begrenzten Modellierung von Bedeutung im Semantic Web[207] auch direkte Anknüpfungspunkte an die allgemeine Forschung zur Künstlichen Intelligenz (KI). Neuere Entwicklungen zum Soft Computing[208] (u.a. Fuzzy Logic, Neuronale Netze, Evolutionary und Chaotic Computing) sind durch ihren „unscharfen", eher der menschlichen Adaptionsfähigkeit und natürlichen Prozessen nachgebildeten Ansatz möglicherweise tragfähiger als die KI-Forschung früherer Jahrzehnte. Andererseits kann man durchaus skeptisch sein, wie weit diese Forschungen wirklich führen und ob es gelingen wird, sie in realen Systemen praktisch umzusetzen.

Zum Kontextverständnis ist eine Sammlung und Speicherung von nutzerbezogenen Informationen in einer neuen Quantität und Qualität notwendig. Eine zentrale Frage, die sich somit automatisch aus der Vision des Calm Computing ergibt und die stark hemmend auf seine Entwicklung wirken kann, ist, ob und wieweit es möglich ist, unter diesen Voraussetzungen die informationelle Selbstbestimmung des Individuums zu bewahren.

3.1.8 Sicherheit der Technik

„*Ubiquitous Interconnectivity = Widespread Vulnerability*"

President's Information Technology Advisory Committee, PITAC (2005, S. 7).

Alle bisher genannten technischen Bestimmungsfaktoren haben auch Einfluss auf die Sicherheit von Ubiquitous Computing-Systemen – im Sinne von Schutz vor Unfällen oder Ausfällen (Safety) und vor Angreifern (Security).[209] Miniaturisierung führt zur Updateproblematik, die zur Verfügung stehende Energie bestimmt die Qualität von einsetzbaren Sicherheitsprotokollen, Interoperabilität und Vernetzung können die Angreifbarkeit der Anwendungssysteme erhöhen, die Gestaltung von Interfaces kann gute oder schlechte Konfiguration von Systemen durch den Menschen zur Folge haben und die Delegation von Funktionen und Kontextverständnis macht besonders die „Safety" der Technik stark abhängig von der Qualität der Modellierung und ihrer adäquaten Reaktion in den zahlreichen Situationen der jeweiligen Anwendungen. Andererseits muss die Sicherheit als Anforderung bereits beim Design von Ubiquitous Computing-Systemen berücksichtigt werden[210], sie ist damit also auch ein Bestimmungsfaktor für seine Entwicklung.

Ranganathan (2004) identifiziert die folgenden zentralen, aber schwer zu lösenden Sicher-

[206] Abowd, 2002, S. 35-38. Detailliert Schmidt, 2002. Davies, 2002, S. 27f.; Tandler, 2001, S. 100.

[207] Zur Vision Berners-Lee, 2000, bes. S. 191ff.

[208] Technischer Überblick z.B. bei Aliev, 2004.

[209] Gutes Fundament bietet Stajano, 2002.

[210] So z.B. Stajano, 2002, S. 82; allgemein Anderson, 2001.

heitsfragen im Pervasive bzw. Ubiquitous Computing:[211]

- Mit wem unterhalte ich mich?
- Wird meine Privatsphäre gewahrt bleiben?
- Kann ich dem Gerät trauen, mit dem ich kommuniziere?
- Gibt es eine Regressmöglichkeit?
- Werden die Dienste zuverlässig verfügbar sein?

Bereits die Frage nach einer zuverlässigen Authentifizierung von Geräten und Nutzern im Ubiquitous Computing erscheint fundamental.[212] Welches Objekt mit anderen „sprechen" darf und welcher Nutzer berechtigt ist, eine derartige Kommunikation auszulösen, ist alles andere als eine triviale Frage. Lösungen lassen sich derzeit allenfalls für begrenzte Räume und definierte Nutzer denken, beschränken damit aber auch gleichzeitig die Entwicklung des Ubiquitous Computing.

Nicht weniger fundamental ist die Frage nach der Verantwortlichkeit für Funktionalitäten im Ubiquitous Computing. Auch drohen neue Formen der Abhängigkeit[213] von der allumgebenden Technik. Aufgrund der Anzahl, Komplexität und Dynamik solcher Systeme sind unvorhergesehene und eventuell nicht vollständig aufklärbare Wechselwirkungen möglich.[214] Verliert sich die Zurechnung für technische Fehler und Missbrauch in einer allgegenwärtigen Unverantwortlichkeit, dann können bspw. etwaige Schäden nicht liquidiert werden.[215] Eine Entwicklung, die die Bereitschaft, Ubiquitous Computing zu nutzen, nicht fördern wird.

Wenn man die zahlreichen Sicherheitsprobleme des heutigen Internets auf Ubiquitous Computing extrapoliert, so scheint ihre zufrieden stellende Lösung im Augenblick nicht absehbar. Sicherheitsfragen haben die Verbreitung des klassischen Internet bisher wenig gehemmt, wohl aber die Entwicklung des E-Commerce B2C[216]. Von einer befriedigenden Lösung der Sicherheitsfragen in Ubiquitous Computing-Systemen im Design, der Implementierung und ihrer Verwendung wird die weitere Entwicklung maßgeblich abhängen.[217]

---

[211] Guter Überblick zur Problematik auch bei Gow/ITU, 2005.

[212] Zu Authentifikation als dringender Forschungsfrage siehe PITAC, 2005, S. 37.

[213] Langheinrich, 2005, S. 9.

[214] Zur Entstehung von Komplexität in großen Systemen mit sogar nur einfachen lokalen Interaktionsregeln siehe z.B. Resnick, 1994.

[215] Siehe näher Kap. 3.4.

[216] TNS-Emnid, 2005, S. LVIf.

[217] PITAC, 2005, gibt neben einem aktuellen Überlick zur Lage der IT-Sicherheit auch Handlungsempfehlungen, die nicht nur für die USA relevant sein dürften.

3.1.9 Literatur

Abowd, Gregory D. / Mynatt, Elizabeth D.: Charting Past, Present, and Future Research in Ubiquitous Computing, ACM Transactions on Computer-Human Interaction, Vol. 7, No. 1, March 2000, S. 29–58.

Aliev, Rafik Aziz / Fazlohalli, Bijan / Aliev, Rashad Rafik: Soft Computing and its Applications in Business and Economics, Studies in Fuzzyness and Soft Computing, Vol. 157, Springer, Berlin, 2004.

Anderson, Ross: Security Engineering – A Guide to Building Dependable Distributed Systems, Wiley, New York, 2001.

Berners-Lee, Tim: Weaving the Web – The Past, Present and Future of the World Wide Web, Texere, London, 2000.

Bush, R. / Meyer, D.: RFC 3439 - Some Internet Architectural Guidelines and Philosophy, 2002, http://ftp.rfc-editor.org/in-notes/rfc3439.txt (21.06.2005).

Cherry, Steven: The Net Effect - IEEE Spectrum Weekly Feature, June 2006, http://www.spectrum.ieee.org/WEBONLY/publicfeature/jun05/0605cnet.html (30.06.2005).

Christensen, Clayton M.: The Innovator's Dilemma, HarperBusiness Essentials, New York 2003.

Davenport, Thomas H. / Beck, John C.: The Attention Economy, Harvard Business School Press, Boston, 2001.

Davies, Nigel / Gellersen, Hans-Werner: Beyond Prototypes: Challenges in Deploying Ubiquitous Systems, IEEE Pervasive Computing, Vol. 1, No. 1, January-March 2002, S. 26-35.

Dertouzos, Michael L.: The Unfinished Revolution: Human-Centered Computers and What They Can Do for Us, HarperCollins, 2001.

Fleisch, Elgar: Ubiquitous Network Societies: Their Impact on the Telecommunication Industry, Background Paper, ITU Workshop on Ubiquitous Network Societies, 2005, http://www.itu.int/osg/spu/ni/ubiquitous/workshop.html (21.06.2005).

Gow, Gordon A.: Privacy and Ubiquitous Network Societies, Background Paper, ITU Workshop on Ubiquitous Network Societies, 2005, http://www.itu.int/osg/spu/ni/ubiquitous/workshop.html (21.06.2005).

Helal, Sumi: Programming Pervasive Spaces, IEEE Pervasive Computing, Vol. 4, No. 1, January-March 2005, S. 84-87.

Helal, Sumi et al.: The Gator Tech Smart House: A Programmable Pervasive Space, IEEE Computer Magazine, March 2005, S. 50-60.

Hilty, Lorenz / Behrendt, Siegfried et al.: The Precautionary Principle in the Information Society – Effects of Pervasive Computing on Health and Environment, Bern, 2005, http://www.empa.ch/sis (20.06.2005).

ISTAG - IST Advisory Group: Ambient Intelligence - From Vision to Reality, 2003, ftp://ftp.cordis.lu/pub/ist/docs/istag-ist2003_consolidated_report.pdf (30.03.2006).

Klaas, Michael: Ableitung von Einflussfaktoren als Grundlage für die Entwicklung von Technologieszenarien im Rahmen der Prognosephase des Technologiemanagements für den Zeitraum 2005-2010, Dissertation, Essen, 2003.

Kurzweil, Ray: The Law of Accelerating Returns, 2001, http://www.kurzweilai.net/meme/frame.html?main=/articles/art0134.html (25.06.2005).

Langheinrich, Marc / Coroama, Vlad / Bohn, Jürgen / Mattern, Friedemann: Living in a Smart Environment – Implications for the Coming Ubiquitous Information Society, Telecommunications Review, Vol. 15, No. 1, February 2005.

Lauterwasser, Christoph: Opportunities and Risks of Nanotechnologies - Report in co-operation with the OECD International Futures Programme, München, 2005, http://www.allianz-azt.de/azt.allianz.de/Industrietechnik/Content/Downloads/Files/Nanotech_dotcom3mb.pdf

(21.06.2005).

Lemley, Mark A. / Lessig, Lawrence: The End of End-to-End - Preserving the Architecture of the Internet in the Broadband Era, UC Berkeley Law & Econ Research Paper No. 2000-19, Stanford Law & Economics Olin Working Paper No. 207; UC Berkeley Public Law Research Paper No. 3, 2001.

Lessig, Lawrence: The Future of Ideas – The Fate of the Commons in a Connected World, Vintage Books, New York, 2002.

Lipp, Lauritz L.: Interaktion zwischen Mensch und Computer im Ubiquitous Computing, LIT, Münster, 2004.

Loshin, Pete: IPv6, Theory, Protocol and Practice, Elsevier, San Francisco, 2004.

Lyytinen, K. / Yoo, Y.: Issues and Challenges in Ubiquitous Computing, CACM 45(12), 2002, S. 62-65.

Mattern, Friedemann: Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing, In: Friedemann Mattern (ed.): Total vernetzt, Springer-Verlag, 2003, S. 1-41.

Mattern, Friedemann: Die technische Basis für das Internet der Dinge, in: Elgar Fleisch, Friedemann Mattern (Eds.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, Springer-Verlag, 2005, S. 39-66.

McCloskey, Paul: From RFID to Smart Dust, a perception of future applications. Presentation, Brussels, 2004, ftp://ftp.cordis.lu/pub/ist/docs/directorate_d/ebusiness/mccloskey_en.pdf (20.06.2005).

Norman, Donald A.: The Invisible Computer, MIT Press, 1999.

Odlyzko, Andrew / Tilly, Benjamin: A refutation of Metcalfe's Law and a better estimate for the value of networks and network interconnections, Preliminary version, March 2, 2005, http://www.dtc.umn.edu/~odlyzko/doc/metcalfe.pdf (20.06.2005).

PITAC - President's Information Technology Advisory Committee: Cyber Security - A Crisis of Prioritization, February 2005, http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf (24.06.2005).

Ranganathan, Kumar: Trustworthy Pervasive Computing: The Hard Security Problems, in: Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), IEEE Computer Society, 2004.

Raskin, Jef: The Humane Interface - New Directions for Designing Interactive Systems, Addison Wesley, 2000.

Resnick, Mitchel: Turtles, Termites, and Traffic Jams – Explorations in Massively Parallel Microworlds, MIT Press, 1994 (Reprint 1997).

Rheingold, Howard: Smart Mobs – The Next Social Revolution, Perseus Books, Cambridge (MA), 2002.

Rogers, Everett M.: Diffusion of Innovations, 5th ed., Free Press, New York, 2003.

Roßnagel, Alexander / Müller, Jürgen: Ubiquitous Computing – neue Herausforderung für den Datenschutz, CR 2004, S. 625-632.

Saltzer, J.H. / Reed, D.P. / Clark, D.D.: End-to-End Arguments in System Design, ACM Transactions on Computer Systems, Vol. 2, No. 4, November 1984, S. 277-288.

Satyanarayanan, M. (ed.): Energy Harvesting & Conservation, IEEE Pervasive Computing, Vol. 4, No. 1, January-March 2005.

Schmidt, Albrecht: Ubiquitous Computing – Computing in Context, PhD Thesis, Lancaster, 2002, http://www.comp.lancs.ac.uk/~albrecht/phd/index.html (24.06.2005).

Shneiderman, Ben / Plaisant, Catherine: Designing the User Interface – Strategies for Effective Human-Computer Interaction, 4th ed., Addison Wesley, 2004.

Stajano, Frank: Security for Ubiquitous Computing, Wiley, Chichester (UK), 2002.

Swann, Peter: Ökonomie der Normung, Manchester, 2000.

Tandler, Peter: Software Infrastructure for Ubiquitous Computing Environments: Supporting Synchronous Collaboration with Heterogeneous Devices, Proceedings of UbiComp 2001: Ubiquitous Computing, Springer LNCS 2201, Heidelberg 2001, S. 96-115.

TNS-Emnid, Monitoring Informationswirtschaft, 8. Faktenbericht, 5. Trendbericht, im Auftrag des Bundeswirtschaftsministeriums, München April 2005.

Weiser, Mark: The Computer for the 21st Century. Scientific American, 265, 3, 1991, S. 66-75.

Weiser, Mark: Some Computer Science Problems in Ubiquitous Computing, Communications of the ACM (CACM), 36(7), July 1993. S. 75-84.

Weiser, Mark / Brown, John Seely: The Coming Age of Calm Technology, 1996, http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm (20.06.2005).

Willinger, Walter / Doyle, John: Robustness and the Internet – Design and Evolution, 2002, http://netlab.caltech.edu/pub/papers/part1_vers4.pdf (20.06.2005).

3.2 Soziale Bestimmungsfaktoren des Ubiquitous Computing

Sarah Spiekermann

3.2.1 Einleitung

Bei der Diskussion sozialer Faktoren im Zusammenhang mit elektronischen Systemen wird heute sehr häufig auf den Aspekt des Datenschutzes fokussiert. Datenschutzbedenken führen, so wird an vielen Stellen argumentiert, dazu, dass viele Konsumenten auf den elektronischen Handel (E-Commerce) verzichten. Im Hinblick auf das Ubiquitous Computing geht man davon aus, dass sich diese Ängste der Menschen vor einem Missbrauch der Technik verschlimmern werden. Dies ist insofern gerechtfertigt, als dass intelligente Umgebungen, so wie sie heute von Wissenschaftlern antizipiert werden, mehr Daten über Menschen und ihre Objekte sammeln können, als dies jemals zuvor der Fall war. Nicht ausgeschlossen werden kann damit auch eine zweckentfremdete Speicherung und Weiterverarbeitung. Einige Wissenschaftler weisen daher heute schon darauf hin, dass das Ubiqutous Computing das Potenzial hat, traditionelle Modelle des Datenschutzes auszuhebeln: „*The most fundamental rules violated by ubiquitous information systems are the Collection Limitation Principle, the Purpose Specification Principle and the Use Limitation Principle*“.[218]

Als Antwort auf diese Entwicklung haben Verbraucherschutzaktivisten in USA[219] und in Deutschland[220] in öffentlichen Aktionen gegen die Einführung von UC, insbesondere der RFID-Technologie, protestiert. Dadurch ist in der Industrie die Sensibilität für die potenziellen sozialen Auswirkungen der UC-Technologien gewachsen. In einer Pro und Contra-Darstellung versuchte z.B. die Harvard Business Review im November 2004 Antworten darauf zu geben, ob es für den Handel empfehlenswert sein kann, RFID auf der Verkaufsfläche einzusetzen, oder ob man lieber davon absehen sollte.[221]

Insgesamt werden die sozialen Auswirkungen des Ubiquitous Computing in den gegenwärtigen Diskussionen in Presse und Wissenschaft gerne ausschließlich auf das Problem der Einbuße von Privatheit reduziert, wobei die Rolle des Menschen als Konsument oder Bürger im Vordergrund steht.

Soziale Auswirkungen und Bestimmungsfaktoren des Ubiquitous Computing sollten jedoch auf einer breiteren Basis diskutiert werden und die unterschiedlichsten Rollen und gesellschaftlichen Austauschbeziehungen mit einschließen, in denen Technologie zum Einsatz kommt. Ferner sollte nicht nur die *informationelle* Selbstbestimmung betrachtet werden,

[218] Cas, 2005, S. 24-33.

[219] Siehe Kathrine Albrecht: http://www.nocards.org/AutoID/overview.shtml

[220] Siehe foebud e.V.: http://www.foebud.org/rfid/

[221] Fusaro, 2004.

wenn soziale Auswirkungen des Ubiquitous Computing diskutiert werden, sondern es sollten auch die Auswirkungen der Technologie(en) auf die *physische* Selbstbestimmung betrachtet werden.

Um das gesamte Spektrum aufzuspannen, in dem informationelle Selbstbestimmung betrachtet werden sollte, bietet sich das Pyramidenmodell von Parsuraman an.[222] Hier wird Technologie im Zentrum eines Spannungsfeldes zwischen Unternehmung, Arbeitnehmer und Konsument gesehen (siehe Abbildung 6).

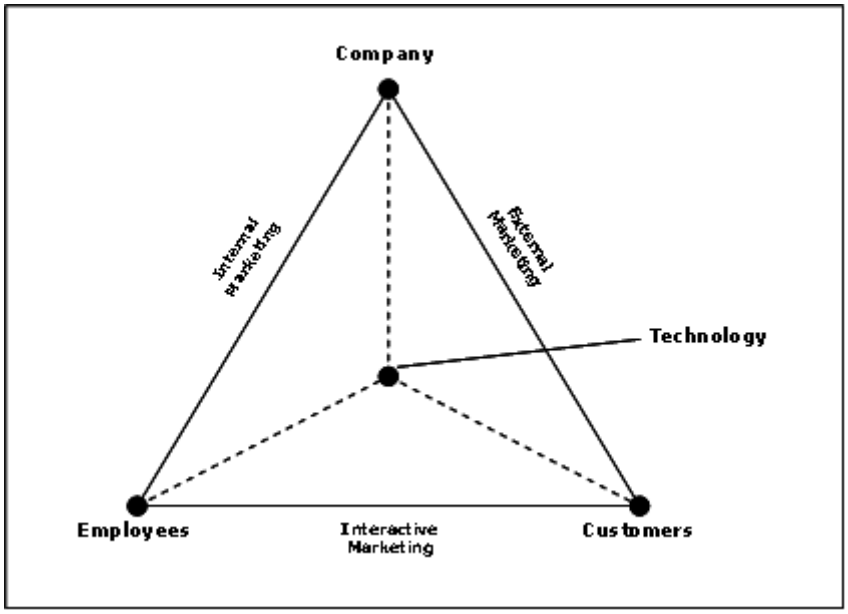


Abbildung 6: Pyramidenmodell nach Parasuraman

Der Arbeitnehmer steht mit seinem Arbeitgeber in einer internen Beziehung, welche von Technologie beeinflusst wird (z.B. E-Mail, Mobiltelefonie). Gleichzeitig steht der Arbeitnehmer in einer Beziehung zum Kunden der Unternehmung und nutzt Technologie, um diese Beziehung zu optimieren (z.B. durch Customer Relationship Management Software). Und schließlich steht die Unternehmung direkt in Beziehung zum Kunden, wenn sie die Kanäle zum Kunden nutzt, die ihr mittels moderner Technologie zur Verfügung stehen (z.B. elektronische Nachrichten, automatisiertes Ticketing).

Soziale Auswirkungen von Ubiquitous Computing sind auf all diesen Beziehungsebenen greifbar. So kam es z.B. zu einem Aufstand von Lastwagenfahrern einer Speditionsgesellschaft, als diese mittels moderner Ortungstechnik prüfen wollte, wo genau sich ihre Fahrer befinden und wie viel Zeit sie auf welchen Streckenabschnitten verbringen. Dieses Anwendungsbeispiel ist nur eines unter vielen, welches die Frage aufwirft, wie stark Unternehmen ihre Mitarbeiter mit UC Technologie überwachen dürfen. Es gibt aber auch noch andere Faktoren, wo Technologie die Beziehung zwischen Arbeitnehmer und Arbeitgeber prägt: Zum

[222] Parasuraman, 2000.

Beispiel etablieren sich Erwartungshaltungen auf Seiten des Arbeitgebers, was Erreichbarkeit und Response-Zeiten angeht oder die aktive Nutzung multipler Endgeräte und Softwarelösungen (nicht nur E-Mail und Telefon, sondern auch Instant Messaging, Webcam, Beeper, Groupware etc.). Gleichzeitig belegen erste wissenschaftliche Arbeiten zum Teil negative Auswirkungen von Technologie auf die Leistungsfähigkeit von Angestellten. So wurde z.B. nachgewiesen, dass das unmittelbare Antworten auf E-Mail Nachrichten zu Produktivitätseinbußen und sogar Intelligenzverlust führen kann.[223] Je nachdem, wie Arbeitgeber Technik im Arbeitsumfeld einsetzten, könnten sich also auf den unterschiedlichsten Ebenen soziale Konsequenzen aus dem Ubiquitous Computing ergeben (Arbeitnehmer – Unternehmung).

Arbeitnehmer stehen, wenn sie an der Kundenschnittstelle tätig sind, häufig in einer Art interaktiven Beziehung zum Kunden. Zum Beispiel, wenn sie Letztere systematisch mit modernen Datamining-Verfahren analysieren, in Vermarktungssegmente einteilen und dann entsprechend adressieren. Je nach Auswirkungen für den Kunden sind solche personalisierten Ansprachen nicht immer einheitlich. Die unkontrollierte Kategorisierung von Menschen wird von vielen Datenschützern kritisiert. Gleichzeitig gibt es aber auch unabhängig vom Datenschutz andere Fragestellungen im Zusammenhang mit UC, wie etwa der bisher freizügige Umgang mit dem knappen Gut der Aufmerksamkeit. Sollen Call-Center-Mitarbeiter auch weiterhin das Recht haben, Kunden zu kontaktieren? Welche Schnittstellen sollten für das interaktive Marketing genutzt werden dürfen? Sollten Kunden umgekehrt das Recht auf eine ‚Mindestansprache' bei Unternehmen haben, auch wenn aufgrund von UC ‚persönliche' Kommunikation relativ teurer wird (Arbeitnehmer – Kunde)?

Schließlich führt insbesondere Ubiquitous Computing zu einer Multiplikation der Informationskanäle und Schnittstellen mit dem Kunden. Und diese Multiplikation ist darüber hinaus durch eine Automatisierung der Schnittstellen gekennzeichnet (Unternehmung – Kunde). Aus sozialer Sicht stellt sich die Frage, in welchem Ausmaß und in welcher Form diese Informationskanäle von Unternehmungen frei genutzt werden sollen und dürfen. Wie darf ein Kunde z.B. im öffentlichen Raum angesprochen werden? Und wie reagiert er auf persönliche Adressierung? Welche Geschäftsmodelle sind ethisch akzeptabel? Bis zu welchem Grad können und sollen Dienstleistungen automatisiert werden dürfen?

Die Zahl der gesellschaftlichen Fragestellungen, die sich durch den breiten Einsatz von Ubiquitous Computing ergibt ist kaum überschaubar. In Kapitel 5 dieses Berichts wird der Versuch unternommen, Chancen und Risiken systematisch und aus Verbrauchersicht zu beleuchten. Dabei stehen zwei wesentliche Bestimmungsfaktoren im Fordergrund, die aus Sicht der Autoren dieser Studie entscheidend dafür sein werden, ob das Ubiquitous Computing aus gesellschaftlicher Sicht wünschenswert bzw. marktfähig ist. Diese beiden Faktoren bestehen einerseits im Erhalt von informationeller, andererseits im Erhalt physischer Selbstbestimmung.

[223] Ahmed, T.: Abuse of technology can reduce UK workers' intelligence - HP calls for more appropriate use of "always-on" technology to improve productivity, HP Press Release. Bracknell, UK, 2005.

Im Folgenden soll die Bedeutung dieser beiden Bestimmungsfaktoren herausgearbeitet werden.

3.2.2 Informationelle Selbstbestimmung im Ubiquitous Computing

Der Erhalt von Privatsphäre (als Ziel des Datenschutzes) spielt nach Meinung von Soziologen eine wichtige Rolle in der Gestaltung zwischenmenschlicher Interaktion, menschlicher Weiterentwicklung und im Erhalt von Demokratie. In Deutschland spiegelt sich das Streben nach dem Erhalt von Privatsphäre rechtlich im Begriff der "informationellen Selbstbestimmung" wieder, welches im Rahmen des Volkszählungsurteils 1982 aus Art. 1 des deutschen Grundgesetzes zur Menschenwürde abgeleitet wurde.

Soziologisch wird der Prozess, mit dem Menschen ihre Privatsphäre schützen oder aufgeben, als eine Art "Grenzverwaltung" verstanden:[224] *„Privacy is an interpersonal boundary-control process, which paces and regulates interaction with others",*[225] schreibt Erwin Altman, einer der Urväter der Privacy-Forschung 1975. Diese Grenzkontrollmechanismen können unterschiedlicher Natur sein. So unterscheiden Bohn et al.[226] im Hinblick auf das Ubiquitous Computing zwischen vier Mechanismen, denen sich der Mensch als Individuum und als Teil eines gesellschaftlichen Systems bedient, um seine Privacy zu gewährleisten. Diese sind:

1. natürliche (physische) Abschottung
2. Vergessen
3. Vergänglichkeit
4. soziale Separierung von Information

Die physische Abschottung, wie etwa das Aufsuchen von einsamen Orten, scheint die naheliegendste Form zum Schutz von Privatsphäre zu sein. Jedoch spielt auch das Vergessen und die Vergänglichkeit von Informationen zur eigenen Person eine Rolle. Wenn wir anderen etwas anvertrauen oder auch schon mal Dinge sagen, die wir nicht wirklich meinen, gehen wir davon aus, dass andere diese Dinge vergessen und uns nicht nachtragen. Wenn dem nicht so ist, und Informationen weiter getragen werden, fühlen wir uns u.U. in unserer Privatsphäre verletzt. Ebenso spekulieren wir auf Vergänglichkeit von Informationen. Äußerungen (oft sogar Handlungen!) in unserer Jugend wollen wir uns nicht über Jahrzehnte nachtragen lassen. Werden uns Dinge, wie z.B. die Zugehörigkeit zu einer radikalen Fußballfangruppe in unseren 20ern, auch nach Jahrzehnten noch vorgehalten oder sogar sanktioniert, fühlen wir uns in unserer Privatsphäre verletzt, da uns auf Basis der Vergangenheit etwas suggeriert

---

[224] Altman, 1975.

[225] Ü.d.A.: Der Erhalt der Privatsphäre ist ein zwischenmenschlicher Grenzkontrollmechanismus, der die Interaktion mit anderen sowohl reguliert als auch zeitlich determiniert. http://www.ejcl.org/83/art83-1.html, http://portal.acm.org/citation.cfm?id=357402, http://proceedings.informingscience.org/IS2002Proceedings/papers/Boyce230Beyon.pdf (30.03.2006).

[226] Bohn et al, 2004.

wird, was wir mit uns in unserer Gegenwart nicht mehr verbinden. Und schließlich die soziale Distanz: Hier gehen wir davon aus, dass unser Handeln in einem sozialen Kontext nicht (fälschlicherweise) auf einen anderen Kontext übertragen wird. Wenn jemand beispielsweise zu einer Prostituierten geht, erwartet er, dass diese Information im Bordellmilieu verbleibt und nicht seinen Arbeitgeber erreicht. Ebenso verhält es sich mit Informationen zu Krankheiten oder ausgefallenen Hobbys, die einen in eine ‚Schublade' hineinschieben könnten, die man für sich selbst nicht anerkennt oder nicht kommunizieren möchte.

Bohn et al. führen nun aus, wie diese Grenzmechanismen durch Ubiquitous Computing außer Kraft gesetzt werden könnten. Durch Ortungstechnik, Videokameras und generell einer Umgebung, die sich des Menschen ‚bewusst' ist und auf diesen reagiert, wird es immer schwieriger sein, sich physisch abzuschotten. Arbeiten von Boyle und Adams zu geteilten Multimedia-Umgebungen verdeutlichen dies: Wenn Mitarbeiter von zu Hause arbeiten und dabei Videokameras einsetzen, die den Kollegen verraten, wo sie sind und was sie machen, ist eine Abschottung im heimischen Arbeitszimmer nicht mehr so einfach möglich.[227] Vor allem dann nicht, wenn Firmenrichtlinien eine aktive Kamera vorsehen. Ebenso ist es bei einem breiten Einsatz von Ortungstechnologie (wie GSM oder GPS) kaum noch möglich, den eigenen Aufenthaltsort zu verbergen, wenn diese zum Zwecke des Flottenmanagements (im Unternehmen) oder Auffinden von Freunden und Kindern eingesetzt werden; insbesondere dann nicht, wenn Arbeitgeber, Freunde oder Eltern erwarten, dass man die eigene Position regelmäßig offen legt.

Vergessen und Vergänglichkeit sind Eigenschaften von Menschen, nicht aber von Datenverarbeitungssystemen. Ist es uns möglich, durch Ortungstechniken, RFID oder Sensoren, menschliche Bewegungsprofile, soziale Netze, Gesundheitszustände, Fahrverhalten etc. ständig aufzuzeichnen (z.B. zum Zwecke der Erbringung bestimmter Dienstleistungen), dann liegt auch das längerfristige Speichern und Auswerten solcher Informationen nahe (sofern dies datenschutzrechtlich erlaubt ist). So ist z.B. offen, wie ein heute aktiver Fußballhooligan, der einmal in der Datenbank ‚Gewalttäter Sport' gelandet ist, dort in den nächsten Jahrzehnten wieder gestrichen werden kann. Im Zweifelsfall wird er vielleicht auch als braver Familienvater in 20 Jahren noch auf die Teilnahme an Fußballspielen verzichten müssen.

Und schließlich soziale Separierung von Informationen: Bei diesem Aspekt der Privatsphäre steht die Verwendung von Informationen im richtigen Kontext im Mittelpunkt der Betrachtung. Ein Fax oder Ausdruck darf nur von dem gelesen werden, für den er bestimmt ist. Ein Einblick ins Telefonierverhalten nur von dem, der die Rechnung stellt. Häufig kommt es jedoch auch heute schon zu einem unkontrollierten Kombinieren von Informationen über Kontexte und ‚Berechtigte' hinweg: Sei es, dass der Kunde durch Überlesen des ‚Kleingedruckten' in eine Vielzahl von Datenverarbeitungsprozessen eingewilligt hat oder dass die Verknüpfung von Informationen grundsätzlich erlaubt ist. So können Daten zweckentfremdet werden. Ein gegenwärtig relevantes Beispiel sind Adressdaten. Wenn diese mit dem Bestellwesen im E-Commerce-System verknüpft werden, hat das zur Folge, dass nur derjenige auf Zahlung per

[227] Adams, 2000; Boyle, 2001; Boyle, 2003.

Nachnahme bestellen kann, der auch im ‚richtigen' Haus in der ‚richtigen' Strasse wohnt. Ob dies den meisten Menschen heute schon bewusst ist, ist derzeit unklar. In UC-Umgebungen könnten sich aufgrund der Masse an verfügbaren Daten die Potenziale einer derart entfremdeten Datennutzung weiter verbreiten.

Dieser Trend zur Zweitverwertung von Daten (auf Englisch: „secondary use"), ebenso wie der zunehmend merkliche Einschnitt in die Privatsphäre aufgrund der Langlebigkeit und Allgegenwärtigkeit von Informationen, führen bei Verbrauchern bereits heute zu einem Gefühl des Kontrollverlusts (siehe Abbildung 7). Um das Jahr 2000 empfanden rund 80% der Befragten in 2 verschiedenen Verbraucherstudien in den USA, dass Konsumenten eine Kontrolle über die Sammlung und Weiterverarbeitung ihrer persönlichen Daten verloren hätten.[228] Gleichzeitig bestätigten 83% der Befragten, dass sie bei einem Unternehmen nicht mehr kaufen würden, wenn bekannt wird, dass dieses sich nicht datenschutzkonform verhält. Die Privacy-Reputation scheint daher ein wichtiger Faktor zu sein, den Unternehmen bei ihrer Datenverarbeitungsstrategie mit berücksichtigen sollten (s.u.).

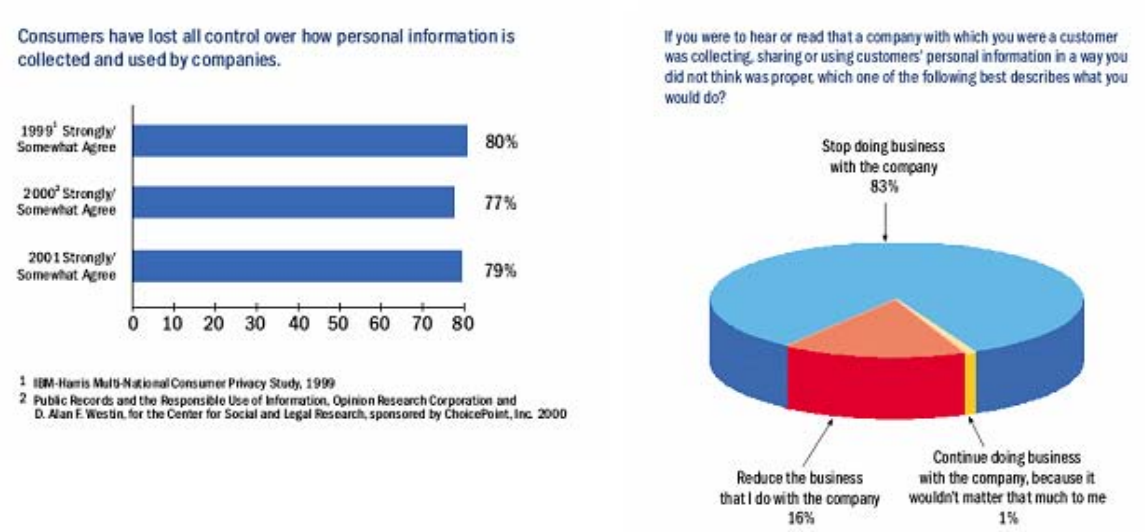


Abbildung 7: Verbraucherbefragung in den USA zum Thema Privacy (nach Ernst & Young, 2002)

Betrachtet man die Aussagen von Verbrauchern, in denen ein sehr hohes Datenschutzbewusstsein und der Wunsch nach Kontrolle zum Ausdruck gebracht werden, so kann man leicht zu dem Schluss kommen, dass die sozialen Kosten in Form eines Verlusts der informationellen Selbstbestimmung als zu hoch empfunden werden. Tatsächlich jedoch belegen einige Studien in Deutschland und in den USA, dass Bedenken in Sachen Datenschutz fast nie zu entsprechend kongruentem Schutzhandeln bei Verbrauchern führen.[229] Wird dem Kunden die Preisgabe seiner Daten im Kontext plausibel gemacht (z.B. Videoüberwachung zur Erhöhung von Sicherheit) oder erhält er sogar einen Vorteil im Gegenzug für die Informationspreisgabe (z.B. Kundenkarten, Empfehlungen), scheinen für die meisten Menschen Datenschutzbedenken an Bedeutung zu verlieren, oder sie sind zumindest nicht mehr hand-

[228] Ernst & Young LLP, Privacy: What Consumers Want. E. Y. A. a. A. B. Services, 2002.

[229] Acquisti / Grossklags, 2005; Berendt / Guenther / Spiekermann, 2005.

lungsrelevant.

Erklärungsansätze dafür, dass Einstellung und Verhalten nicht konsistent sind, besagen, dass Menschen dazu neigen, kumulative Risiken zu unterschätzen. So könnte es sein, dass sie auch die langfristige Speicherung ihrer Daten und die daraus potenziell entstehende ‚historische Aussagefähigkeit' unterschätzen. Alternativ kann es sein, dass die meisten Menschen de facto heute einfach noch zu wenig über die Datenverarbeitung wissen, um diese in ihren Auswirkungen richtig zu begreifen. Hier könnte eine entsprechende Aufklärung viel Positives bewirken.

Durch die Einführung von Ubiquitous Computing wird es – das zeigen viele Kapitel dieses Berichts – zu einer Potenzierung der Sammlung und Verarbeitung persönlicher Daten kommen. Die Ausführungen in diesem Kapitel zeigen ferner, dass dadurch die informationelle Selbstbestimmung bzw. die Privatheit auf vielen Ebenen bedroht ist. Die Frage, die sich stellt ist, ob diese Bedrohung von den Bürgern auch wahrgenommen wird, wie diese zu informationsintensiven Diensten stehen, inwieweit sie auf das Vorhandensein von „schützenden" Gesetzen vertrauen und unter welchen Bedingungen sie der Datenverarbeitung zustimmen. Wichtig ist auch zu verstehen, welche relative Bedeutung dem Wunsch nach Privatsphäre zukommt, wenn dieser anderen Nutzen- und Kostenelementen der Entscheidungsfindung gegenüber gestellt wird. Nur ein besseres Verständnis dieser Zusammenhänge und Fragestellungen erlaubt es zu beurteilen, ob Datenschutzbedenken in Deutschland zu einem ernsthaften Hindernis bei der Einführung von Ubiquitous Computing-Dienstleistungen führen können und wo die Dienste technisch und prozessual entsprechend angepasst werden sollten, um auf die Akzeptanz des Marktes zu stoßen.

Kapitel 5 dieses Berichts unternimmt daher einen Versuch, erste Antworten auf diese Fragen zu finden. Hier wird über die Erwartungen und Einstellungen von über 5.000 Teilnehmern einer empirischen Studie berichtet, die im Rahmen des TAUCIS-Projekts durchgeführt worden ist.

3.2.3 Physische Selbstbestimmung im Ubiquitous Computing

Wie anfangs beschrieben beinhaltet das UC neben dem Datenschutz noch weitere soziale Bestimmungsfaktoren. Einer davon, das postulieren die Autoren dieser Studie, besteht in der *physischen* Selbstbestimmung des Menschen in einer intelligenten Umgebung. Im Kern geht es dabei um die Kontrolle des Menschen über seine Objekte, wenn diese mit intelligenter Reaktionsfähigkeit ausgestattet werden bzw. autonom und im Hintergrund Entscheidungen für ihre Besitzer treffen. Marc Weiser beschreibt die Problematik in seinem Leitartikel zum Ubiquitous Computing wie folgt:[230] „The [social] problem [associated with UC], while often couched in terms of privacy, is really one of control."

Wenn Objekte intelligent werden und auf Menschen automatisch reagieren, gibt es einen schmalen Grad, auf dem der Nutzenvorteil eines Dienstes gegen ein Gefühl des Kontrollver-

[230] Weiser, 1991.

lustes und der Bevormundung abgewogen werden muss. Ein gutes Beispiel sind Warntöne bei Nichtanschnallen im Auto: Mittels Sensoren stellt das Auto fest, dass der Fahrer nicht angeschnallt ist und zwingt diesen daraufhin durch ein entsprechendes Warnsignal, den Schutzgurt im eigenen Interesse anzulegen. Der Nutzenvorteil dieses UC-Dienstes liegt einerseits auf der Hand: Die Anschnallpflicht des Fahrers wird technisch durchgesetzt und die Verletzungsgefahr desselben dadurch reduziert. Andererseits gibt es viele Menschen, die das Signal als negative Bevormundung empfinden und vielleicht sogar bewusst einen Wagen ohne diese Funktionalität kaufen möchten.

Durch die allgegenwärtige Verfügbarkeit von Sensoren und RFID-Chips sowie entsprechende „Intelligenz" in den Produkten besteht die Möglichkeit, dass ähnliche Funktionalitäten auf breiter Front entwickelt und in Produkte implementiert werden. Die Möglichkeiten der Technik können dazu genutzt werden, die Menschen darauf zu kontrollieren, ob und wie sie Regeln und Gesetze befolgen. Dies wirft insbesondere dann Probleme auf, wenn derjenige, der die Technik zu verantworten hat, unbestimmte und konkretisierungsbedürftige Rechtsregeln einseitig in seinem Sinne auslegt und über die Ausrichtung des technischen Systems den Betroffenen „seine Auslegung" aufzwingt. Dort, wo diese Möglichkeiten der Technik genutzt werden, um Gesetze zu zementieren, wird es zu einem Verlust von „Grauzonen" im Umgang mit gesetzlichen Vorschriften kommen und es steht den Autoren dieses Berichts nicht zu, diesen Verlust zu bewerten.

Fraglich ist jedoch, welchen Erfolg Hersteller haben werden, die vergleichbare Funktionen in ihre Produkte einbauen wollen. Sicherlich gibt es für Produkthersteller ökonomische Anreize, den Gebrauch von und Umgang mit den von ihnen vertriebenen Gütern stärker zu kontrollieren. Ein Beispiel ist die Koppelung von Produkten an ihre Accessoires, wie etwa eine Bohrmaschine, die nur noch in Betrieb genommen werden kann, wenn der Heimwerker eine entsprechende Schutzbrille von demselben Hersteller trägt[231], der CD-Spieler, der CDs nur noch abspielt, wenn diese legal erworben wurden (bzw. über einen entsprechenden Lizenzcode verfügen), ein Auto, was nur noch anspringt, wenn der Fahrer nachweisen kann, dass er nicht getrunken hat[232] etc. In all diesen bereits existierenden Anwendungen wird dem Menschen die Kontrolle über seine Produkte entzogen. Die Frage ist jedoch, ob eine solche Nutzung des Ubiquitous Computing, die kurzfristig attraktiv erscheinen mag, langfristig erfolgreich sein kann. Ganz abgesehen davon, dass ein solcher „Technologiepaternalismus" sicherlich gesellschaftlich nicht wünschenswert sein kann[233], stellt sich auch die Frage, ob er marktfähig ist.

Vor diesem Hintergrund postulieren wir, dass der Grad der Kontrolle, den Menschen über UC-Produkte und Dienstleistungen haben werden, ein wesentlicher Bestimmungsfaktor für ihre Akzeptanz sein wird. Wobei Akzeptanz im zweiten Schritt auch Vermarktungserfolg be-

[231] Elektrisierende Idee", Technology Review – Das M.I.T Magazin für Innovation, Nr. 5, 2005, S. 30.

[232] Saab: Saab unveils Alcohol Lock-Out Concept to discourage drinking and driving, Saab South Africa, 2005. Online: http://www.saab.com/main/ZA/en/alcokey.shtml (27.04.2005).

[233] Spiekermann / Pallas, 2005.

deutet und die Fähigkeit zur Schaffung marktnaher Produktinnovationen. In Kapitel 5 dieses Berichts wird diese Hypothese empirisch anhand einer Verbraucherstudie nachgewiesen, die im Rahmen des TAUCIS-Projekts durchgeführt worden ist. Hier wurden vier verschiedene UC-Anwendungen von Verbrauchern bewertet, wobei der Grad der Kontrolle über dieselben experimentell variiert wurde. Es zeigt sich dabei, dass mehr Nutzerkontrolle eindeutig zu einer höheren Kauf- und Nutzungswahrscheinlichkeit führt.

Allerdings kann die wahrgenommene Kontrolle über UC-Anwendungen nicht isoliert betrachtet werden. Sie ist zum einen abhängig von der jeweiligen Umgebung des Verbrauchers und zum anderen nicht der einzige Faktor, welcher die Akzeptanz der neuen Produktlandschaften bestimmt. Aus der Territorialitätsforschung ist beispielsweise bekannt, dass Heimatterritorien mit größerer Kontrollierbarkeit assoziiert werden als fremde bzw. öffentliche Territorien.[234] Daher ist zu erwarten, dass ein Verzicht auf Kontrolle im öffentlichen Raum eher akzeptiert wird als im privaten Umfeld. Ein weiterer wichtiger Faktor, der die Wirkung der wahrgenommenen Kontrolle beeinflusst, ist das Eigentum am Gegenstand. Wir gehen davon aus, dass Gegenstände, die sich in unserem Eigentum befinden, vom Besitzer eher vollständig kontrolliert werden wollen als öffentliche Objekte.[235] Wird die Kontrolle über einen Gegenstand eingeschränkt, so resultiert bei eigenen Produkten eine stärkere Tendenz, dieser Kontrollbeschränkung entgegenzuwirken, als wenn der Gegenstand uns nicht gehört.

Schließlich steht Kontrolle oder die physische Selbstbestimmung sicherlich in einem Spannungsverhältnis zu anderen Faktoren, die für die Akzeptanz eines UC-Dienstes bedeutsam sind. So gibt es sicherlich Szenarien, in denen Menschen ihre physische Selbstbestimmung gerne aufgeben, wenn sie dadurch andere, höher geschätzte Vorteile erlangen. So könnte UC-Technik beispielsweise genutzt werden, um heute vorhandene Risiken zu reduzieren. Wieder ist der Anschnallgurt im Auto ein gutes Beispiel: Für viele Fahrer, die das physische Risiko, ohne Gurt zu fahren, als besonders hoch einschätzen, mag das Warnzeichen eine willkommene Hilfsfunktion beim sicheren Fahren darstellen. Wahrgenomme Risiken und die Möglichkeit, diese durch UC-Technik zu reduzieren, könnten also einen wichtigen Gegenpol zur Kontrolle bilden, wenn es um die Beurteilung der neuen Dienstleistungen geht.

Und schließlich spielen sicherlich auch solche Faktoren eine Rolle bei der Akzeptanz von Ubiquitous Computing, welche in der klassischen Technologieakzeptanzforschung behandelt werden. Diese postuliert, dass es insbesondere die wahrgenommene Nützlichkeit eines Dienstes ist sowie die wahrgenommene Einfachheit ihrer Bedienung, die ausschlaggebend für die Akzeptanz sind.[236]

Zusammenfassend lässt sich sagen, dass die Autoren dieses Berichts die positive soziale Einbettung des Ubiquitous Computing in unseren Alltag davon bestimmt sehen, inwieweit es gelingt, UC-Dienste so zu gestallten,

---

[234] Altman, 1975.

[235] Siehe Pierce / Kostova / Dirks, 2003.

[236] Davis / Bagazzi et al., 1989.

- dass sie den Erwartungen der Verbraucher an ihre informationelle Selbstbestimmung gerecht werden,
- dass sie im Sinne einer physischen Selbstbestimmung dem Verbraucher ausreichend Kontrolle über die intelligenten, reaktionsfähigen Infrastrukturen und Objekte belassen und
- dass sie nützlich und einfach zu bedienen sind, wobei diese Nützlichkeit auch davon abhängt, inwieweit ein Dienst in der Lage ist, heute bestehende relevante Nutzungsrisiken von Verbrauchern zu reduzieren.

3.2.4 Literatur

Abramson, L. Y. / Seligman, M. E. P. / Teasdale, J. D: Learned Helplessness in Humans: Critique and Reformulation, Journal of Abnormal Psychology, Vol. 87, 1978.

Acquisti, A. / Grossklags, J.: Privacy and Rationality in Individual Decision Making, IEEE Security & Privacy, 2005, 2, S. 24-30.

Adams, A.: Multimedia information changes the whole privacy ballgame, Computers, Freedom and Privacy CFP 2000, San Francisco, USA.

Adams, J. S.: Inequity in social exchange, Advances in Experimental Social Psychology, Vol.2, 1965, S. 12-38.

Ahmed, T.: Abuse of technology can reduce UK workers' intelligence - HP calls for more appropriate use of "always-on" technology to improve productivity, HP Press Release, Bracknell, UK, 2005.

Altman, I.: The environment and social behavior: Privacy, personal space, territory, crowding, Monterey, California, Brooks/Cole, 1975.

Averill, J. R.: Personal control over aversive stimuli and its relationship to stress, Psychological Bulletin, Vol. 80, 1973.

Bandura, A.: Human agency in social cognitive theory, American Psychologist, Vol. 44, 1989, S. 1175-1184.

Berendt, B. / Guenther, O. / Spiekermann S.: Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, Communications of the ACM 48(4), 2005.

Bohn, J. / Coroama, V. et al.: Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications, Journal of Human and Ecological Risk Assessment 10(5), 2004.

Boyle, M.: Ubiquitous Awareness Spaces Calgary, Alberta, Canada, Department of Computer Science, University of Calgary, 2001.

Boyle, M.: A Shared Vocabulary for Privacy, Fifth International Conference on Ubiquitous Computing, Seattle, Washington, 2003.

Brehm, S. S. / Brehm, J.: Psychological Reactance: A Theory of Freedom and Control, San Diego, 1981.

Brehm, J. W.: A Theory of psychological reactance, New York, Academic Press, 1966.

Butler, J. K.: Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory, Journal of Management, Vol. 17, 1991, S. 643-663.

Cas, J.: Privacy in Pervasive Computing Environments - A Contradiction in Terms?, IEEE Technology and Society 24(1):, 2005, S. 24-33.

Cook, J. / Wall, T.: New Work Attitude Measures of Trust, Organizational Commitment, and Personal Need Nonfulfillment, Journal of Occupational Psychology, Vol. 53, 1980, S. 39-52.

Davis, F.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, MIS Quarterly 13(3), 1989, S. 319-340.

Davis, F. / Bagozzi, R., et al.: User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, Management Science 35(8), 1989, S. 982-1003.

Deutsch, M.: The effect of motivational orientation upon trust and suspicion, Human Relations, Vol. 13, 1960, S. 123-140.

Ernst & Young LLP, Privacy: What Consumers Want. E. Y. A. a. A. B. Services, 2002.

Ferster, C. B.: A functional analysis of depression, American Psychologist, 28 (10), , 1973, S. 857-870.

Fusaro, R.: None of Our Business, Harvard Business Review, 2004, S. 33-44.

Guenther, O. / Spiekermann, S.: RFID and Perceived Control - The Consumer's View, Communica-

tions of the ACM, September 2005.

Gefen, D.: E-commerce: the role of familiarity and trust, The International Journal of Management Science, Vol. 28, S. 725-737.

Hong, S. M. / Faedda, S.: Refinement of the HPRS, Educational and Psychological Measurement, 56, 2996.

Hong, S. M. / Page, S.: A psychological reactance scale: Development, factor structure and reliability. Psychological Reports, Vol. 64, 1989, S. 1323-1326.

Jones, A. P. / James, L. R. / Bruni, J. R.: Perceived Leadership Behavior and Employee Confidence in the Leader as Moderated by Job Involvement. Journal of Applied Psychology, Vol. 60, 1975, S. 146-149.

Kang, J. / Cuff, D.: Pervasive Computing: Embedding the Public Sphere, Public Law & Legal Theory Research Paper Series, Los Angeles, US, University of California, Los Angeles School of Law, 62, 2005.

Lazarus, R. S. / Folkman, S.; Stress, appraisal, and coping, New York, 1984.

Lewinsohn, P. M.: A behavioral approach to depression, in Friedmann, R. J. / Katz, M. M. (Eds.), Psychology of Depression, Contemporary Theory and Research, Oxford: John Wiley & Sons, 1974, S. 157-178.

Mayer, R. C. / Davis, J. H. / Schoorman, F. D.: An integrative model of organizational trust, Academy of Management Review, Vol. 20, 1995, S. 709-734.

Mehrabian, A. / Russell, J. A.: An Approach to Environmental Psychology, MIT Press, 1974.

Merz, J.: Fragebogen zur Messung der Psychologischen Reaktanz [Questionnaire for Measuring Psychological Reactance], Diagonistica, 29, 1983, S. 75-82.

Parasuraman, A: Technology Readiness Index (TRI) - A Multiple-Item Scale to Measure Readiness to Embrace New Technologies, Journal of Service Research 2(4), 2000, S. 307-320.

Pierce, J. L. / Kostova, T. / Dirks, K. T.: The State of Psychological Ownership: Integrating and Extending a Century of Research, Review of General Psychology, Vol. 7, 2003, S. 84-107.

Rotter, J. B.: Generalized Expectancies for interpersonal trust, American Psychologist, 35, 1971, S. 1-7.

Seligman, M. E. P.: Helplessness: On Depression, Development, and Death, San Francisco, Freeman, 1975.

Spiekermann, S. / Pallas, F.: Technology Paternalism - Wider Implications of RFID and Sensor Networks, Poiesis & Praxis - International Journal of Ethics of Science and Technology Assessment 4, 2005.

Spiekermann, S. / Ziekow, H.: RFID: a 7-point plan to ensure privacy. In: 13th European Conference on Information Systems, ECIS, Regensburg, 2005.

Venkatesh, V.: Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model, Information Systems Research 11(4), 2000, S, 342-365.

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

Wortman, C. B. / Brehm, J.: Responses to uncontrollable outcomes: An integration of reactance theory and the learned helplessness model, In L. Berkowitz (Ed.), Advances in experimental social psychology Vol. 8, New York: Academic Press, 1975. S. 277-336.

3.3 Ökonomische Bestimmungsfaktoren des Ubiquitous Computing

Kai Dingel, Michael Klafft, Sarah Spiekermann

3.3.1 Einleitung

Die Grundidee des Ubiquitous Computing (UC) wird bereits seit Ende der 80er Jahre diskutiert[237]. Marktfähige UC-Lösungen werden jedoch in großem Stil erst seit wenigen Jahren angeboten, so zum Beispiel in der Logistik (RFID) oder im Bereich der ortsbasierten Dienste (Location Based Services).

Zurzeit ist noch unklar, welche wirtschaftliche Bedeutung die vielfältigen Anwendungen des Ubiquitous Computings in ihren einzelnen Märkten erlangen werden. Um eine frühzeitige Abschätzung der technischen und ökonomischen Weiterentwicklung zu ermöglichen, sollen im Folgenden die für die Zukunft des UC relevanten ökonomischen Bestimmungsfaktoren diskutiert werden. Wir trennen dabei zwischen der Nachfrage- und der Angebotsseite.

3.3.2 Bestimmungsfaktoren auf der Nachfrageseite

3.3.2.1 Endverbraucher als Nachfrager von Ubiquitous Computing

Grundvoraussetzung für den Erfolg eines neuartigen Informations- und Kommunikationssystems ist die Akzeptanz durch die Nachfrager, die Benutzer. Nach Davis[238] wird diese entscheidend bestimmt von dem wahrgenommenen Systemnutzen (der so genannten „Usefulness“) und der Benutzerfreundlichkeit („Ease of Use“) der neuen Technologie. Ein weiterer wichtiger Aspekt für den Erfolg neuer Technologien und Dienste ist das Vertrauen, dass die Nutzer den neuen Produkten entgegenbringen.

3.3.2.1.1 Der Systemnutzen (Usefulness)

Systemnutzen in der ursprünglichen Definition[239] bezeichnet die vom Anwender wahrgenommene Verbesserung der Arbeitsleistung aufgrund des Einsatzes eines Informationssystems. Diese einseitige Fokussierung auf die Kenngröße Arbeitsproduktivität greift im Ubiquitous Computing-Umfeld jedoch zu kurz, da die hiermit verbundenen Informationssysteme zum Bestandteil des Alltagslebens werden und auch private Freizeitaktivitäten immer stärker durchdringen werden. Das Modell der Technologieakzeptanz von Davis muss daher um emotionale Faktoren erweitert werden.[240] Dies sind (in Anlehnung an Amberg / Wehrmann, 2003):

---

[237] Weiser et al., 1999.

[238] Davis, 1989.

[239] Davis, 1989, Chan, 2001.

[240] Malhotra / Galetta, 1999.

- „Status“ als soziales Herausstellungsmerkmal
- „Spaß“ als hedonistisches Motivationselement
- Förderung von Kommunikation und Interaktion als soziokulturelles Motivationselement
- Verwirklichung persönlicher Freiheit (libertaristisches Motivationselement)

Zusammen mit dem bereits von Davis identifizierten Elementen der Zeitersparnis, der Effizienzsteigerung und Flexibilisierung bilden diese Faktoren den Mehrwert einer UC-Technologie bzw. eines UC-Dienstes für den Endnutzer.

Der wahrgenommene Nutzen der neuen Lösung wird dabei bestimmt von der Effizienz und Leistungsfähigkeit der derzeitigen Lösung sowie dem Potential der besten, dem Nutzer bekannten Alternativlösung. Die Effizienz von Ubiquitous Computing-Anwendungen ist in diesem Zusammenhang geprägt von der Fähigkeit zur situativen Adaptivität. Kontextbezogene Informationen müssen erfasst, ausgewertet und zur Bereitstellung individualisierter Dienstebündel genutzt werden. Bei Beurteilung von Leistungsfähigkeit und Alternativen spielt auch die Bepreisung des Dienstes eine wichtige Rolle. Diese muss aus Endkundensicht in einem angemessenen Verhältnis zum Nutzen stehen.

3.3.2.1.2 Der Bedienkomfort (Ease of Use)

Die Bedeutung des (wahrgenommenen) Bedienkomforts für den Erfolg neuartiger Technologie ist bereits seit langem bekannt (so Rockart, 1987, in Bezug auf Informationssysteme).

Bedienkomfort bedeutet, dass jederzeit und überall eine einfache, effiziente und effektive Durchführung der Systemaktivitäten gewährleistet sein muss.

Für die Entwicklung des Ubiquitous Computing ist dieser Faktor besonders wichtig, da es sich hierbei um Systeme handelt, die ein breites, nicht technikorientiertes Publikum ansprechen sollen. Ziel ist dabei nicht nur die ubiquitäre Verfügbarkeit, sondern auch die weitgehende Unsichtbarkeit der Systeme.[241]

Hieraus lassen sich drei Unterziele für die Erreichung des größtmöglichen Bedienkomforts ableiten:

- Anwendungsfreundlichkeit (Usability, umfasst die ergonomische, intuitive Gestaltung der Benutzerschnittstellen);
- Interoperabilität (im Sinne von Plattform-, Software- und Kontextinteroperabilität)[242];
- Minimaler Aufmerksamkeitsbedarf (Attention, im Sinne des Calm Computing weitgehender Verzicht auf Benutzerinteraktion durch Autokoordination und Autoorganisation).

Vor dem Hintergrund der zunehmenden Knappheit der Ressource Aufmerksamkeit ist zu erwarten, dass die Bedeutung des „Ease of Use“ in Zukunft noch an Bedeutung gewinnen und somit einen Schlüsselfaktor für den Erfolg von Ubiquitous Computing-Anwendungen

[241] Gupta / Moitra, 2004.

[242] Strang, 2003.

darstellen wird.

3.3.2.1.3 Vertrauen (Trust)

Ein weiterer wichtiger Faktor für die Servicewahl ist das subjektive Vertrauen des Konsumenten in den jeweiligen Diensteanbieter (so Chan / Gillenson / Sherrell, 2004, in Bezug auf E-Commerce). Wichtig für das Kundenvertrauen im Ubiquitous Computing ist, wie oben beschrieben, der Glaube daran, dass Unternehmen zuverlässig, vorhersehbar, kompetent und integer sind in der Art und Weise wie sie UC-Anwendungen zur Verfügung stellen.

Diese das Vertrauen bestimmenden Unterfaktoren beziehen sich zum einen auf den Datenschutz, zum anderen aber auch auf den Dienst selbst.

Im Hinblick auf den Datenschutz sind unter anderem folgende Fragen relevant:

- Welche Kontrolle hat der Nutzer über die Datenerhebung?
- Welche Kontrolle hat der Nutzer über die Datennutzung?
- Erfolgt eine Lokalisierung des Konsumenten - wenn ja von wem und zu welchem Zweck?
- Wie, wo und wie lange werden die erhobenen Daten gespeichert?
- Wie werden die Daten ausgewertet?
- Welche technischen und organisatorischen Voraussetzungen wurden getroffen, um Verletzungen des Datenschutzes zu verhindern?
- Wird die Privatsphäre des Anwenders respektiert (nicht intrusive Dienste)?
- Welche Anbieter und Partner stehen hinter den jeweiligen Dienstleistungen und wie ist das jeweilige Markenimage?

Im Hinblick auf die Dienstbereitstellung ist zu bemerken, dass das Ubiquitous Computing durch seine technischen Eigenschaften ökonomische Potenziale eröffnet, die für Unternehmen zwar durchaus attraktiv sein können, aus Verbrauchersicht jedoch nicht unbedingt wünschenswert sind.[243] So könnten Produkte beispielsweise in Abhängigkeit von der Nutzungsintensität bepreist werden. Es könnten Produktbündel technisch forciert werden. Oder bestimmte Nutzungsformen, wie etwa der Weiterverkauf einer Fußballkarte auf dem Schwarzmarkt, könnten unterbunden werden. Hier ist es jedoch für Unternehmen erforderlich zu hinterfragen:

- Erfüllt die Dienstequalität die grundlegenden Kosten- und Nutzenerwartungen der Konsumenten?
- Welche Tarifmodelle werden vom Nutzer als gerecht empfunden?
- 'Verhalten' sich Systeme in einer vorhersehbaren und als fair empfundenen Art und Weise?

Darüber hinaus beinhaltet die ‚Unsichtbarkeit' in der UC-Technik die Notwendigkeit, dass

[243] Spiekermann / Pallas, 2005.

sich Kunden bedingungslos auf diese verlassen können. Das heißt, dass bei der Markteinführung neuer UC-Lösungen sehr hohe Anforderungen an die Verfügbarkeit (availability) und Sicherheit (security) zu stellen sind. Fehler- und Ausfallquoten, wie sie bei gegenwärtigen Softwarelösungen heute häufig der Fall sind, sind dann nicht mehr tragfähig.

Wie gut es Unternehmen gelingt, ihre Kompetenz, Integrität und Zuverlässigkeit nicht nur marketingtechnisch zu signalisieren, sondern auch praktisch einzuhalten, wird bestimmend dafür sein, wie sich die Lösungen im Einzelnen durchsetzen. Der Staat kann die Bildung von Vertrauen und somit die Technologieakzeptanz durch datenschutz- und verbraucherfreundliche normative Rahmenbedingungen unterstützen. Gefordert sind vor allem aber die Anbieter von Ubiquitous Computing-Systemen, deren Marktchancen von der Akzeptanz der Anwender abhängig sind.

3.3.2.2 Unternehmen als Nachfrager von UC-Technologie

3.3.2.2.1 Bedarf an neuartigen Informations- und Kommunikationssystemen

Die rasante Verbreitung und Weiterentwicklung ubiquitärer Dienste und Lösungen wird signifikante Auswirkungen auf die Arbeitswelt der Zukunft haben.

Die zunehmende Miniaturisierung von IT-Hardware sowie die Weiterentwicklung natürlicher Benutzerschnittstellen wird es ermöglichen, Informationssysteme in Umgebungen einzusetzen, in denen sie zurzeit aufgrund technischer oder wirtschaftlicher Restriktionen nicht verwendet werden können - wie etwa bei vielen Tätigkeiten mit hohem manuellen Arbeitsanteil.

In Zukunft werden zum Beispiel kooperative Arbeitsumgebungen (CSCW, Computer Supported Cooperative Work) nicht nur im administrativ-planerischen Umfeld anzutreffen sein, sondern auch verstärkt Eingang in die produktiven Bereiche der Unternehmen finden. Ubiquitäre IT-Systeme bieten in der Produktion grundsätzlich folgende Vorteile (teilweise in Anlehnung an Skattør et al. 2004):

- Verbesserte Möglichkeiten zur Kommunikation und Kooperation,
- Unmittelbare Überbrückung von Diskontinuitäten,
- Statuserfassung von Mitarbeitern,
- Unterstützung von Dokumentationsprozessen in der Qualitätssicherung oder bei der Produktrückverfolgung,
- Unterstützung von Suchprozessen (zum Beispiel nach Material und Bauteilen),
- Bereitstellung von Situationsinformationen in dynamischen Umgebungen,
- Nutzung von Echtzeittransparenz in der Prozesssteuerung,
- Durchführung von Ferndiagnosen und Fernwartung (bis hin zur Fehlerantizipation),
- Steigerung des Automatisierungsgrads durch Förderung von Autokoordination und Autoorganisation.

Besondere Relevanz wird diesen IT-basierten Unterstützungsleistungen bei der Herstellung

von Produkten zukommen, die besonderen Dokumentationsanforderungen genügen müssen (z.B. Luftfahrzeuge), aufgrund ihrer physikalischen Größe aber nicht oder nur zu geringen Teilen automatisiert gefertigt werden können (z. B. Schiffe, Luftfahrzeuge, Druckmaschinen, Gebäude) oder eine extreme Typen- und Variantenvielfalt aufweisen (z.B. Druckmaschinen).

Neben der Unterstützung von Produktionsprozessen durch ubiquitäre Informations- und Kommunikationssysteme sehen Entwicklungsszenarien insbesondere eine zunehmende Verbreitung des Ubiquitous Computing im Logistik-Bereich voraus.

Auto-ID-Technologien wie etwa RFID ermöglichen hier eine weitergehende Automatisierung (zum Beispiel am Point of Sale) bei gleichzeitig verbesserter Informationserfassung in sich dynamisch verändernden Umgebungen.

3.3.2.2.2 Akzeptanz bei den Mitarbeitern

Die Einführung von UC-Technik wird trotz aller eingangs genannten Potenziale wesentlich bestimmt werden von der Akzeptanz, auf die diese bei Mitarbeitern trifft. Kann, z.B. durch die RFID-Technik, auf vielen Stufen der Wertschöpfung Personal eingespart werden, so ist nicht auszuschließen, dass sich Mitarbeiter gegen die Einführung wehren wollen und die Einführung boykottieren. Ebenso kann es auf Basis von UC-Technik potenziell zu mehr Überwachung von einzelnen Mitarbeitern kommen, insbesondere kann die individuelle Arbeitsleistung genauer nachvollzogen werden. Obgleich dies grundsätzlich nichts Neues ist (Akkordlohn gibt es ja schon seit fast 100 Jahren), ist die Akzeptanz der Mitarbeiter aus unserer Sicht ein wesentlicher Bestimmungsfaktor für die Einführung und den Erfolg der Technologie. Diese Akzeptanz kann nicht durch den Aspekt der Kosteneinsparungen erzielt werden, sondern muss sich auf andere Qualitäten der UC-Technologie stützen, die glaubhaft kommuniziert werden müssen. Dazu gehören die erhöhte Wettbewerbsfähigkeit deutscher Unternehmen, die verbesserte Produktqualität, ein erhöhter Verbraucherschutz (z.B. durch das Nachvollziehen von Lieferketten) oder vereinfachte Prozessabläufe für Arbeitnehmer selbst.

3.3.2.2.3 Vertrauen zwischen den Marktteilnehmern

Neben der Mitarbeiterakzeptanz ist Echtzeittransparenz von Prozessen nicht immer etwas, was sich alle Partner entlang einer Wertschöpfungskette wünschen. Im Rahmen von ECR-Initiativen (Efficient Consumer Response) wurde in den letzten Jahren sehr viel mehr Transparenz in den Warenstrom hinein gebracht. Jedoch spielt hier das Vertrauen zwischen den Marktteilnehmern und die Bereitschaft Echtzeitdaten auszutauschen eine große Rolle. Nur wenn Anreize gefunden werden können, die ein Profitieren aller Wertschöpfungspartner von der Technologie gewährleisten, ist eine volle Ausschöpfung der Vorteile von UC-Technologie absehbar.

3.3.2.2.4 Lösung technischer Probleme

Schließlich sind für die breite Nutzung der UC-Technik einige wesentliche technische Hürden zu nehmen. Dazu gehört im Bereich Logistik insbesondere die Lösung von Einleseproblemen. Immer noch haben beispielsweise RFID-Infrastrukturen zu hohe Fehlerraten, um für einen breiten Einsatz auf Einzelproduktebene geeignet zu sein. Die Zuverlässigkeit der Systeme ist daher auch hier bestimmend für die Einführbarkeit.

3.3.2.2.5 Trade-off zwischen Sicherheit und Kosten

Ist die Technik einmal eingeführt, so ist eine langfristige Nutzung in vielen Branchen sicherlich auch abhängig von dem Grad der Sicherheit, den diese zu einem adäquaten Kostenniveau bietet. Immerhin ist die Information über Warenströme wirtschaftlich sensibel. Sind Systeme zu leicht angreifbar, wie dies z.B. bei der RFID-Technik derzeit immer noch stark diskutiert wird, so ist nicht auszuschließen, dass sich einzelne Branchen gegen eine breite Nutzung entscheiden oder zumindest die Einsatzgebiete beschränken.

3.3.2.2.6 Standardisierung

Schließlich ist für die Nutzung von ökonomischen UC-Potenzialen die Standardisierung der Technik und der damit verbundenen Nummernstandards entscheidend. Im Bereich RFID sind hier insbesondere die Standardisierungsgremien der GS1 (früher in Deutschland CCG) zu nennen, die international sowohl Leseinfrastrukturen als auch Datenaustauschformate vorantreiben.

3.3.3 Bestimmungsfaktoren auf der Angebotsseite

3.3.3.1 Kooperation und Konzentration

Während der individuelle und industrielle Technologienutzen einen wesentlichen Treiber für die Nachfrage darstellt, sind in einer Marktwirtschaft die Gewinnchancen der an der Wertschöpfung von UC-Diensten beteiligten Unternehmen ebenso ausschlaggebend für die Entwicklung eines entsprechenden Technologieangebots.

Eine Besonderheit des UC Technologie besteht darin, dass kaum durchgängige Wertschöpfungsketten für Produkte und Dienste bestehen. Mehrwert entsteht vielmehr aus dem aufeinander abgestimmten, synergetischen Zusammenspiel einzelner komplementärer Wertschöpfungsebenen: der Hardwareebene, der Zugangsebene, der Anwendungsebene und der Inhaltsebene.

In den Markt für Dienste des Ubiquitous Computing treten viele etablierte Unternehmen ein, die sich aufgrund bestehender Ressourcen, bestehender Infrastruktur oder bereits erworbenen Wissens durch einen komparativen Vorteil auf einer dieser Ebenen auszeichnen. Sie nutzen Breitenvorteile zu ihren bestehenden Geschäftsfeldern aus, decken jedoch selten die gesamte Bandbreite des vom Kunden nachgefragten UC-Produkt- oder Dienstebündels ab.

Etablierte Unternehmen verfügen zum Teil über erhebliche Marktmacht und haben daher häufig relativ hohe Margenerwartungen. Im Bereich des Ubiquitous Computing führt dies derzeit dazu, dass die von den Kunden nachgefragten Dienstekombinationen oft zu hoch bepreist werden und kaum Abnehmer finden. Die Anbieter befinden sich in einem Gefangenendilemma: Ihre subjektiv optimalen Entscheidungen führen objektiv zu suboptimalen Marktergebnissen. Ein gutes Beispiel sind mobile Datendienste wie etwa die Location-based Services.

Ein Bestimmungsfaktor ist daher, inwieweit es den Marktteilnehmern der unterschiedlichen

Ebenen gelingen wird, so zu kooperieren, dass eine marktfähige Endkundenlösung angeboten werden kann.

Ein in der Praxis hierbei häufig gegangener Weg ist die verstärkte Konzentration von Diensten und Produkten – und zwar ebenenübergreifend. Aus Unternehmenssicht bietet diese Integration Vorteile, da durch Akquisition von Schlüsselressourcen und –technologien die Errichtung und Ausweitung von Markteintrittsbarrieren begünstigt wird. Beispielsweise versuchen viele Hersteller von Softwareapplikationen diese durch attraktive und exklusive Inhalte aufzuwerten. Man denke etwa an das mobile ‚Lara Croft'-Handyspiel. Langfristige Schutzrechte (Patente und Marken) zementieren diese Konzentration.

Aus gesamtwirtschaftlicher Sicht bergen solche Produktbündelungen die latente Gefahr, dass technisch zweitklassige Lösungen eine dominierende Marktstellung erreichen. Sind solche inferioren Lösungen erst einmal etabliert, so wird ihre Dominanz aufgrund vorherrschender Netzwerkeffekte noch weiter verstärkt. Technisch überlegenen Alternativlösungen ist es dann nur schwer möglich, einen signifikanten Marktanteil zu gewinnen.

Ebenenübergreifende Konzentrationsprozesse sowie langfristige Schutzrechte könnten die Entwicklung von attraktiven UC Diensten durch junge und weniger kapitalintensive mittelständische Unternehmen erschweren. Eine Verlangsamung der Marktentwicklung, an vielen Stellen weniger attraktive Diensteangebote und das Ausscheiden vieler kleinerer Unternehmen könnten die Folge sein.

3.3.3.2 Ubiquitous Computing als Differenzierungsmedium

Das ubiquitäre Rechnen ermöglicht die Erfassung zusätzlicher Kundenparameter und die zeitnahe Bereitstellung und Nutzung dieser Informationen an nahezu jedem Ort. Die über ein Individuum zur Verfügung stehende Datenmenge wird daher in Zukunft sowohl an Breite als auch an Aktualität gewinnen. Hieraus ergeben sich für die Unternehmen ökonomisch interessante Differenzierungsmöglichkeiten:[244]

- Höhere Servicedifferenzierung durch gezieltere Identifikation von attraktiven Kunden[245].
- Produktdifferenzierung: Unterbreitung „maßgeschneiderter" Angebote (up-selling oder cross-selling).
- Preisdifferenzierung: Ermittlung und Ausnutzung der (vermuteten) Zahlungsbereitschaft des Kunden durch individuelle Preissetzung (ggf. mit geringfügiger Variation des Produkts).
- Individuellere Risikoabschätzung: Durch das UC zusätzlich gewonnene Informationen ermöglichen im Kredit-[246] und Versicherungswesen[247] eine noch individuellere Bestim-

[244] In Anlehnung an Spiekermann et al., 2003.

[245] Zur Kundensegmentierung siehe auch Boyce, 2002.

[246] Vgl. Aalbers, 2004.

[247] Vgl. Filipova / Welzel, 2005.

mung von Kundenrisiken und Risikoprämien.

Diese Differenzierungsansätze werden es den Leistungsanbietern erlauben, zusätzliche Umsätze zu generieren, die Produzentenrente zu steigern und Kosten und Risiken zu verringern. Erweiterte Möglichkeiten zur Produkt-, Preis- und Servicedifferenzierung stellen daher einen wichtigen Treiber für die Nutzung und Weiterentwicklung des ubiquitären Rechnens durch die gewerbliche Wirtschaft dar.

3.3.3.3 Investitionsrisiken

Investitionen in Informationssysteme zeichnen sich im Regelfall durch ein hohes bis sehr hohes Risiko aus, da es sehr schwierig ist, die Kosten und den Nutzen einer Systemeinführung oder Systementwicklung ex-ante zuverlässig zu bestimmen. Diese Schwierigkeiten sind darin begründet, dass indirekt wirkenden Faktoren und Effekte häufig einen dominierenden Einfluss auf den wirtschaftlichen Erfolg bzw. Misserfolg eines Systems haben. Auf Kostenseite zählen zu den indirekten Effekten beispielsweise: [248]

- Kosten für die Inanspruchnahme des Managements durch das IT-Projekt,
- Kosten für die Beseitigung von Fehlfunktionen und Funktionsstörungen,
- Kosten notwendiger Reorganisationsmaßnahmen (Business Process Reengineering),
- Belastungen der organisatorischen Ressourcen (und daraus eventuell folgende Produktivitätseinbußen) und
- Kosten, die durch verdeckte, nicht antizipierte Widerstände gegen die Einführung/Nutzung des IT-Systems verursacht werden.

Die Herausforderung bei der Ermittlung des Systemnutzens besteht darin, auch monetär nicht quantifizierbare Nutzeneffekte adäquat zu berücksichtigen und mit den monetären Effekten zu einer Gesamtbewertung zusammenzufassen. Zur Lösung dieser Problematik sind verschiedene mehrdimensionale Bewertungsverfahren verfügbar. In der Praxis erwiesen sich diese jedoch als nur bedingt aussagekräftig (wie etwa Scoring-Modelle) oder als schwer handhabbar (wie etwa der Analytic Hierarchy Process), so dass Investitionsentscheidungen häufig auf einer unsicheren Entscheidungsgrundlage getroffen werden.

Investitionen in Informationssysteme und Informationstechnologien finden darüber hinaus in einem sich besonders dynamisch entwickelnden Umfeld statt. Die zu entwickelnden Systeme unterliegen daher einem besonders hohen technologischen Veralterungsrisiko. Zahlreiche zum Zeitpunkt des Investitionsentscheids getroffene Annahmen sind bei der Einführung des Systems möglicherweise schon wieder obsolet, so dass das System sich u. U. nicht wie geplant entfalten kann.

Wie spekulativ Investitionen in Informationssysteme tatsächlich sind, zeigt die folgende Tabelle, in der für typische Arten von Systemen die durchschnittliche Wahrscheinlichkeit aufge-

[248] Vgl. Remenyi et al., 2000, S. 90-94.

führt ist, mit der die jeweilige Investition zu einem Gewinn führt.

Tabelle 4: Wahrscheinlichkeit eines Gewinns bei Investitionen in IT-Systeme[249]

Art des Systems	**Wahrscheinlichkeit eines Gewinns**
Infrastruktursysteme	50%
Systeme mit direkter Nutzenwirkung	90%
Systeme mir indirekter Nutzenwirkung	50%
Systemimplementierungen aus wettbewerblicher Notwendigkeit	20%
Systemimplementierung mit dem Ziel organisatorischer Veränderungen	50%
Strategische Systeme	50%
Vorgeschriebene Systeme (zur Erfüllung behördlicher Auflagen)	20%
USP: System als einzige Problemlösung	75%

Wie aus Tabelle 1 hervorgeht, sind Investitionen in IT-Systeme ohne direkte Nutzenwirkung hochspekulativ. Zu dieser Kategorie gehören alle diejenigen UC-Systeme, bei denen sich kein direkt quantifizierbarer transaktionaler Mehrwert ergibt. Dies führt zum einen dazu, dass die Zahl der potentiellen Investoren für derartige Systeme begrenzt sein dürfte (eine Wiederholung der „New Economy“-Blase ist unwahrscheinlich), zum anderen werden die verbleibenden Investoren hohe Risikoprämien fordern, wenn der Nutzen eines UC-Systems nicht klar auf der Hand liegt.

Die (zum Teil) ungewissen Kosten-/Nutzen-Relationen von UC-Systemen dürften sich insgesamt hemmend auf die zukünftige Entwicklung des ubiquitären Rechnens auswirken, da für Anwendungen mit indirekten Nutzenwirkungen der Zugang zu privatem Kapital sehr stark eingeschränkt ist.

3.3.3.4 End-to-End-Prinzip bei Dienstarchitekturen

Neben der wertschöpfungsübergreifenden Konzentration von Leistungen durch etablierte Unternehmen wird voraussichtlich darüber hinaus die Architektur zukünftiger Dienste eine wesentliche Auswirkung auf den Innovationsprozess im Ubiquitären Computing haben.

Dabei könnte insbesondere die Aufrechterhaltung der End-to-end-Architektur eine entscheidende Rolle spielen: Das End-to-end-Argument (e2e) wurde erstmals 1981 von Jerome Sal-

[249] In Anlehnung an Lucas, 1999, S. 179f.

zer, David Clark und David Reed propagiert [SCR81]. Es besagt zunächst technisch, dass Rechenfunktionen eher nicht auf unteren Schichten ausgeführt werden sollten (also auf der Netzwerkebene), sondern auf höheren Applikationsschichten. Lawrence Lessig greift dieses Argument 2001 in seinem Buch ‚future of ideas' [Les01] auf. Darin argumentiert er, dass der hohe Grad an Innovation im Internet u.a. auf das e2e-Prinzip zurückzuführen ist, da es jedem Besitzer eines Rechners die Möglichkeit gibt, ‚erfinderisch' tätig zu sein. Lessig plädiert daher für „einfache Netzwerke und intelligente Anwendungen" (S. 34 in [Les01]). Als Beispiel führt Lessig das Innovationstempo im klassischen Telefonnetz an und vergleicht dieses mit der Innovationsgeschwindigkeit im Bereich des Internets. Lessig kommt zu dem Schluss, dass der im Internet beobachtete Innovationsboom hauptsächlich durch das End-to-end-Prinzip getrieben gewesen sei.

Ein wesentlicher Bestimmungsfaktor für die Entwicklung des Ubiquitären Computing ist, ob, und wenn ja, wie eine Aufrechterhaltung des e2e-Prinzip auch im Ubicomp gewährleistet werden kann. Gegenwärtige Bestrebungen, Endgeräte nur noch minimal mit Applikationen auszustatten und stattdessen von zentralen Diensten abhängig zu machen, den Zugang zu mobilen Datendiensten auf das Portal des jeweiligen Mobilfunkanbieters (und seiner Partner) zu reduzieren (z.B. Vodafone life!, i-mode), Ortung von Endgeräten vom Netzwerk abhängig zu machen (A-GPS anstelle von GPS) oder das in Betrieb nehmen von eigenen Endgeräten von einer Authentifizierung abhängig zu machen, sind Entwicklungen, die einem unabhängigen und freien Betrieb von ‚End'-Geräten widersprechen. Ebenso sind Technologien wie RFID und Sensornetzwerke per Definition von einem Netzwerk abhängig, da sie selbst (noch!) nicht genügend Energie und Prozessorleistung besitzen, um unabhängig vom Netzwerk nutzbar zu sein.

Zielt man auf einen intensiven Wettbewerb und einen hohen Innovationsgrad ab, so ist die Aufrechterhaltung des End-to-end-Prinzips als ein wesentlicher Erfolgsfaktor zu betrachten.

3.3.4 Literatur

Aalbers, M. B.: „The Quantified Consumer“ or How Financial Institutions Value Risk, ENHR Conference, Cambridge, 2004.

Amberg, M. / Wehrmann J..: Effizientes Angebot von situationsabhängigen mobilen Diensten, Zeitschrift Industrie Management, Nr. 06, 2003, S. 35-38.

Boyce, G,: Beyond Privacy – The Ethics of Customer Information Systems, Informing Science InSITE 2002, http://proceedings.informingscience.org/IS2002Proceedings/papers/Boyce230Beyon.pdf (18.5.2005).

Chan, S. C.: Understanding adoption and continual usage behaviour towards internet banking services in Hong Kong, Lignan University, October 2001.

Chen, L. / Gillenson, M. L. / Sherrell, D. L.: Consumer Acceptance of Virtual Stores: A theoretical Model and Critical Success Factors for Virtual Stores, ACM SIGNIS Database Vol. 35, Issue 2, 2004, S. 8-31.

Davis, F. D.: Perceived Usefulness, perceived Ease of Use, and User Acceptance of Information Technology, MIS Quarterly, Vol. 13 No. 3, Sept. 1989, 319-340.

Filipova, L. / Welzel, P.: Reducing Asymmetric Information in Insurance Markets: Cars with Black Boxes, Volkswirtschaftliche Diskussionsreihe Beitrag Nr. 270, Universität Augsburg, 2005.

Fleisch, E.: Von der Vernetzung von Unternehmen zur Vernetzung von Dingen, 2001.

Gupta, P. / Moitra, D.: Evolving a pervasive IT infrastructure: a technology integration approach, Personal and Ubiquitous Computing 8, 2004, S. 31-41.

Lucas, Henry C. Jr.: Information Technology and the Productivity Paradox – Assessing the Value of Investing in IT, Oxford University Press, New York 1999.

Malhotra, Y. / Galletta, D. F.: Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation, Proceedings of the 32nd Hawaii International Conference on System Sciences 1999.

Mattern, F.: Wireless Future: Ubiquitous Computing, Proceedings of Wireless Congress 2004, Munich, Germany, November 2004.

Remenyi, Dan / Money, Arthur / Sherwood-Smith, Michael / Irani, Zahir: The effective measurement and management of IT costs and benefits (2nd edition), Butterworth-Heinemann, Oxford et al. 2000.

Rockart, J. F.: The Changing Role of the Information System Executive: A Critical Success Factors Perspective, in: Madnick, S. E. (ed.), The Strategic Use of Information Technology, Sloan Management Review – The Executive Bookshelf, Oxford et al. 1987, S. 69-83.

Schmidt-Belz, B.: Aspects of User Trust in mobile guides, Workshop HCI in mobile guides, Udine September 2003, http://www.comp.lancs.ac.uk/computing/users/kc/mguides03/ Schmidt-Belz-final.pdf

Spiekermann, Sarah / Pallas, F.: Technology Paternalism – Wider Implications of RFID and Sensor Networks, Poiesis & Praxis - International Journal of Ethics of Science and Technology Assessment, Springer Verlag, Volume 4, Herbst 2005.

Spiekermann, S. / Dickinson, I. / Günther, O. / Reynolds, D.: User Agents in E-Commerce Environments: Industry vs. Consumer Perspectives on Data Exchange, in Eder, J. und Misikoff, M. (eds.), CAiSE 2003, LNCS 2681, 2003, S. 696-710.

Skattør, B. / Hasvold, P. / Berntzen, L. / Engvig, T.: Mobile Work – Mobile ICT Supporting Secondary Work, INF5260 Final Report, May 2004.

Strang, T.: Service-Interoperabilität in Ubiquitous Computing Umgebungen, Dissertation, LMU München 2003.

Weiser, M. / Gold, R. / Brown, J. S.: The origin of ubiquitous computing research at PARC in the late 1980s, IBM systems journal Vol. 38 Nr. 4, 1999, S. 693-696.

3.4 Rechtliche Bestimmungsfaktoren des Ubiquitous Computing

Jan Möller, Johann Bizer

3.4.1 Einführung

Im Gutachten über die Modernisierung des Datenschutzes aus dem Jahr 2001 werden die datenschutzrechtlichen Auswirkungen des Ubiquitous Computing erstmals problematisiert. Die Autoren beschreiben die Risiken, identifizieren die Defizite des geltenden Datenschutzrechts und schlagen schließlich de lege ferenda eine Differenzierung zwischen einer Datenverarbeitung mit und ohne einem gezielten Personenbezug vor.[250] Die datenschutzrechtliche Debatte hat diese Vorschläge bislang nur unzureichend gewürdigt. Das Gutachten war in diesen Passagen noch zu visionär – die Anwendungen noch zu unwirklich. Immerhin hat in der Zwischenzeit die Datenschutzdiskussion Bedeutung und Auswirkungen des Themas RFID rezipiert und nachvollzogen.[251] Die Aneignung und Auseinandersetzung mit der Bedeutung und den Auswirkungen des Ubiquitous Computing beginnt erst jetzt.

3.4.2 Rechtsrelevante Charakteristika beispielhafter Anwendungsfelder

Das Recht besteht aus Regelsätzen, die das Zusammenleben von Menschen steuern sollen. Zur leichteren Anwendbarkeit und zur Herstellung größerer Rechtssicherheit werden diese Regelungen für konkrete Situationen ausdifferenziert. Daraus ergibt sich für die Entwicklung rechtlicher Bestimmungsfaktoren einer zukünftigen Entwicklung die Notwendigkeit, die geltenden Rechtsvorschriften in einem realen oder zumindest unmittelbar bevorstehenden Anwendungsumfeld des Ubiquitous Computing beispielhaft anzuwenden, um beschränkende oder befördernde Effekte des geltenden Rechts erkennen zu können.

Bei einer solchen Rechtsanwendung spielt die Ausgestaltung der Beispiele eine wichtige Rolle.[252] Die Annahme bestimmter Tatsachen kann das Ergebnis der Rechtsprüfung in gänzlich unterschiedliche Richtungen beeinflussen. Um die Vielzahl der Faktoren kontrolliert einsetzen und so möglicherweise auch bedeutende Ergebnisdifferenzen bei einer nur kleinen Variation eines Beispiels aufzeigen zu können, werden die Anwendungsumfelder im Hinblick auf rechtsrelevante Charakteristika beschrieben.

Folgende Kontextinformationen über *Anwendungsumfelder* sind von besonderer Relevanz

[250] Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts 2001, S. 17, 24, 30, 44, 65, 117.

[251] Siehe bspw. die Entschließung der Konferenz der Datenschutzbeauftragten vom 25./26. März 2004 zu RFID, DuD, 2004, S. 204.

[252] Siehe Kapitel 2, auch die Szenarienbildung in Rossnagel/Müller, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR, 2004, S. 625 (626f.).

für die rechtliche Beurteilung.[253]

- In welchem *Umfeld* handeln beteiligte Personen (z.B. an der Haustür, am Telefon etc.)?
- In welcher *Rolle* handeln beteiligte Personen (z.B. als Verbraucher, für ein Unternehmen etc.)?

Neben diesen Einsatzkontexten sind einige Faktoren der technischen Umsetzung von Funktionalität im konkreten *Beispiel* relevant für die rechtliche Beurteilung:

- Welche eigenen *Handlungen* gehen von den Personen aus (z.B. handelt die Person selbst, nimmt sie etwas passiv wahr oder ist sie ohne Wissen und unbeteiligt an bestimmten Vorgängen?)

Je nach Gestaltung der Technik hat der Nutzer von Ubiquitous Computing verschiedene *Einflussmöglichkeiten* auf die Ergebnisse der Technikanwendung und den damit einhergehenden Verarbeitungsprozessen.

Ubiquitous Computing arbeitet in vielen Fällen mit *Hintergrundsystemen*, die die Verarbeitung und Auswertung erhaltener Informationen übernehmen und damit ein wichtiges Bindeglied zwischen Kontextanalyse und Aktivitätsauslösung darstellen. Die Vernetzung solcher Systeme eröffnet viele Möglichkeiten, aber auch Gefahren für den Nutzer.[254]

Während die (Primär-)Funktionalität einer Anwendung des Ubiquitous Computing und seine Ergebnisse häufig für den Nutzer erkennbar sein dürften, ist die technische Umsetzung dieser Funktionalität meist komplex und für den Betroffenen nicht *erkennbar*. Für die rechtliche Beurteilung ist das Wissen um den Fluss und die einzelnen Schritte der Verarbeitung personenbezogener Daten von entscheidender Bedeutung.

Die Beschreibung der Beispiele aus den folgenden Arbeitsumfeldern sollen in erster Linie Informationen über die oben dargestellten Einflussfaktoren geben.

3.4.2.1 Umfeld: Arbeit

Das Arbeitsumfeld bestimmt einen wesentlichen Anteil der Lebenszeit der Beschäftigten. Dabei sind sie in mehr oder weniger flexible Organisationsstrukturen eingebunden, auf deren Gestaltung sie in der Regel nur begrenzt Einfluss nehmen können.[255] Veränderungen durch den Wechsel des Arbeitsplatzes sind zwar möglich, aufgrund ihrer Bedeutung für den Lebensunterhalt und je nach Arbeitsmarktlage ist diese Option aber nur die Ausnahme. Die Bedingungen und Strukturen des Arbeitsplatzes werden vom Arbeitgeber vorgegeben, dem in erster Linie an der Effektivität und Produktivität des Unternehmens gelegen sein wird. In

[253] Ähnliche Einflussfaktoren beschreibt SWAMI: Scenario Analysis and Legal Framework – First Results, S. 11ff., die auf Grund des über „privacy“ hinausgehenden Blickwinkels dieser Studie ergänzt und untergliedert wurden.

[254] Vgl. Holznagel / Bonnekoh, Radio Frequency Identification – Innovation vs. Datenschutz?, MMR, 2006, S. 17 (19f.).

[255] SWAMI: Scenario Analysis and Legal Framework – First Results, S. 7f.

diesem Zusammenhang kann der Einsatz von Systemen des Ubiquitous Computing im Rahmen des Direktionsrechts des Arbeitgebers ein wichtiges Gestaltungselement des Arbeitsplatzes sein.[256]

Als Ausgleich zu den Arbeitgeberinteressen bietet das Arbeitsrecht den Arbeitnehmern die Möglichkeit zur Mitbestimmung, um akzeptable Arbeitsbedingungen für alle Beteiligten zu schaffen. Eine rechtliche Bindung des Einzelnen kann sich einerseits aus Anweisungen des Arbeitgebers, andererseits aus Instrumenten des kollektiven Arbeitsrechts (Tarifvertrag, Betriebsvereinbarung) ergeben.

In der Arbeitswelt sind daher für die Entwicklung des Ubiquitous Computing nicht nur die das Individuum schützenden datenschutzrechtlichen Vorgaben[257], sondern vor allem auch kollektivarbeitsrechtliche Regelungen als Bestimmungsfaktoren von Bedeutung.[258] Bestimmungen zum Schutz der Arbeitsumgebung/Arbeitsumwelt, z.B. der Arbeitschutz sowie Vorgaben zu Informations- und Telekommunikationsdiensten, die im Rahmen des Arbeitsverhältnisses eingesetzt werden (Telefon, E-Mail, WWW-Nutzung möglicherweise auch zu privaten Zwecken, Telearbeit), können den Einsatz von Ubiquitous Computing im Arbeitsumfeld ebenfalls beeinflussen.

3.4.2.1.1 Beispiel Produktionsprozess

Ein bereits marktreifes Beispiel für den Einsatz von Techniken des Ubiquitous Computing im Arbeitsumfeld ist die Nutzung von RFID zur Steuerung von Vorgängen im Produktionsprozess. Durch die Möglichkeit einer eindeutigen Identifizierung jedes einzelnen Gegenstandes können einzelne Arbeitsschritte automatisiert gesteuert werden, z.B. die Lackierung eines Gegenstandes in einer bestimmten Farbe. Auf dieselbe Weise kann durch eine gezielte Steuerung einzelner Gegenstände verhindert werden, dass unpassende Teile einander nicht zugeordnet und montiert werden (Qualitätsmanagement). Die Speicherung der einzelnen Verarbeitungsschritte eindeutig identifizierter Objekte ermöglicht es, individuelles Fehlverhalten auf einzelne Mitarbeiter und deren Tätigkeit zurückzuführen.[259] Treten an dem Produkt erst später Fehler auf, dann würde das System eine rückwirkende Fehleranalyse durchführen können. Ubiquitous Computing ermöglicht mit anderen Worten, die Arbeitsleistung der Mitarbeiter nach Quantität und Qualität permanent auszuwerten.

Die verschiedenen Zwecke des Einsatzes des Ubiquitous Computing (z.B. zur automatisierten Maschinensteuerung einerseits und zur Mitarbeiterkontrolle andererseits) könnten orga-

[256] Vgl. Däubler, Computersysteme im Handel – rechtliche Rahmenbedingungen für den Betriebsrat, S. 33 (36).

[257] Barthel, RFID-Anwendungen im Betrieb und bei Arbeitnehmerdaten, DANA, 03/2004, S. 5-9.

[258] Zur Gliederung des Arbeitsrechts s.u. Kap. 3.4.3.2.1 und Schaub, Handbuch des Arbeitsrechts, § 2, Rn. 2ff.

[259] Zur Überwachungsfunktionalität von RFID siehe auch Eisenberg, Puschke, Singelnstein, Überwachung mittels RFID-Technologie, ZRP, 2005, S. 9.

nisatorisch und technisch durch Konzepte der Pseudonymisierung getrennt werden.[260] Notwendige Voraussetzung ist aber eine entsprechende Technikgestaltung durch den Arbeitgeber. Dabei spielen die Hintergrundsysteme des Ubiquitous Computing für die Auswertung der erfassten Informationen eine zentrale Rolle. Eine Risikominimierung im Wege einer datenschutzfreundlichen Technikgestaltung könnte im Rahmen der Mitbestimmung über eine Leistungs- und Verhaltenskontrolle von den Betriebsräten angestoßen und eingefordert werden. Voraussetzung ist allerdings, dass den Beschäftigten die dem Ubiquitous Computing zugrunde liegenden Verarbeitungsprozesse ihrer personenbezogenen Daten bekannt sind.

3.4.2.1.2 Beispiel Logistikkette

Als Paradebeispiel für Rationalisierungseffekte durch RFID gilt der Anwendungsbereich der Logistik.[261] Durch die Ausstattung von Einzelprodukten mit RFID werden diese stückweise identifizierbar. Dadurch lassen sich beispielsweise „Fehlversendungen" vermeiden, Diebstähle feststellen und einem konkreten Umfeld zuordnen. Soweit einzelne Mitarbeiter für bestimmte Abschnitte der Logistik verantwortlich sind, lassen sich über die zentralen Hintergrundsysteme Rückschlüsse auf das Arbeitsverhalten ziehen. So könnte z.B. eine gehäufte Anzahl von defekten Produkten einer Lieferung auf ein nicht normgemäßes Verhalten der hierfür verantwortlichen Fahrer bei der Auslieferung schließen lassen. Darüber hinaus ermöglichen automatisiert erfasste Auslieferungszeiten Rückschlüsse über die Effektivität der Fahrer, möglicherweise aber auch über zu hohe Fahrgeschwindigkeiten. Die Kopplung mit Standortdaten könnte darüber hinaus ein Bewegungsprofil der Mitarbeiter[262] ermöglichen (z.B. Auslieferung von Containern auf dem Hafengelände).

Die Einflussmöglichkeiten der Mitarbeiter in der Logistikkette auf solche Auswertungen über Systeme des Ubiquitous Computing sind gering, da sie in erster Linie in Hintergrundsystemen ablaufen, die nicht nur unternehmensintern sondern über die ganze Logistikkette hinweg arbeiten. Die Kontrollmöglichkeiten reduzieren sich, wenn diese personenbezogenen Prozessdaten in Drittstaaten und damit außerhalb der Reichweite der EG-Datenschutzrichtlinie verarbeitet werden. Eine rechtliche Beherrschung dieser Risiken auf der Basis einer kollektivrechtlichen Mitbestimmung oder individualrechtlicher Maßnahmen aus Datenschutz- und Arbeitsrecht setzt eine ausreichende Information der Beschäftigten über die Verarbeitungsprozesse ihrer Daten voraus. Soweit die Prozesskette in einem Hintergrundsystem des Unternehmens verarbeitet wird, sind Maßnahmen des Datenschutzes über Regeln der Zweckbindung sowie durch eine technisch-organisatorische Begrenzung der Mitarbeiterkontrolle möglich.

---

[260] Zur Bedeutung von Pseudonymisierungskonzepten im UC-Umfeld siehe Roßnagel, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR, 2004, S. 625 (631).

[261] Siehe Kapitel 2.

[262] Siehe auch für andere standortbezogene Anwendungen Heise Newsticker: Bundesdatenschützer will keine gläsernen Autofahrer, http://www.heise.de/newsticker/meldung/71439 (29.03.2006).

3.4.2.2 Umfeld: Konsum

Im Konsumumfeld wird Ubiquitous Computing derzeit vor allem zur Realisierung einer nutzerfreundlichen, aber für den Anbieter kostengünstigen Servicedienstleistung eingesetzt. Zum Beispiel können über automatisierte Umsatzlisten der Nachschub organisiert, das Warensortiment auf die Kundenwünsche zugeschnitten und die Erreichbarkeit der Produkte optimiert werden.[263]

Darüber hinaus lässt die kundenbezogene Auswertung von Kauf- und Aufmerksamkeitsdaten (für welche Produktbereiche hat sich der Kunde besonders interessiert?) den Zuschnitt von individuellen Angeboten und Dienstleistungen und eine Steuerung der Kauferfahrung zu. Eine solche Auswertung eines konkreten Kaufverhaltens ermöglicht bei wiederholten Einkäufen eine differenzierte Bildung von Nutzerprofilen, aus denen sich neben dem Einkaufsverhalten auch noch andere Präferenzen wie bspw. die Zahlungsart offenbaren.[264] Diese Informationen lassen direkte Rückschlüsse[265] bspw. auf für den Konsum zur Verfügung stehende Geldbeträge (Schnäppchenjäger, Hochpreissegmentkunde) zu oder können sehr einfach für eine Kundenauswertung anhand von statistischen Wahrscheinlichkeitswerten (sog. Scoring)[266] weiterverarbeitet werden. Der Kunde könnte sich derartigen Auswertungen letztlich nur durch den Verzicht auf Produkte und Dienstleistungen derartiger Anbieter entziehen. Eine Verhaltenssteuerung, die mit zunehmender Verbreitung solcher Auswertungsmethoden nahezu aussichtslos ist.

Betrifft Ubiquitous Computing Personen in ihrer Eigenschaft als Verbraucher, dann sind die besonderen verbraucherrechtlichen Anforderungen an die Gestaltung der mit dem Konsumvorgang verbundenen Prozesse zu beachten. Weitere Bestimmungsfaktoren ergeben sich aus dem Datenschutzrecht, da die Auswertung von Kundenverhalten und eine Profilbildung in das Recht des Kunden auf informationelle Selbstbestimmung eingreifen. Das Umweltrecht liefert zur Belastung der Kunden durch Elektrosmog Vorgaben, da in einem umgrenzten Verkaufsraum eine Vielzahl auf Funk[267] basierender Informationsübertragungen stattfinden werden.

3.4.2.2.1 Beispiel: Shop

Die Verwendung von RFID im Shopumfeld[268] ist durch ein reales Testgeschäft, den Metro-

---

[263] Vgl. auch SWAMI: Scenario Analysis and Legal Framework – First Results, S. 9ff.

[264] Roßnagel / Müller: Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR, 2004, S. 625 (626).

[265] Vgl. Hülsmann: RFIDs – Bleibt der Datenschutz auf der Strecke?, DANA, 04/2004, S. 11-15.

[266] Zum Scoring vgl. Möller / Florax, Datenschutzrechtliche Unbedenklichkeit des Scoring von Kreditrisiken? NJW, 2003, 2724; ULD, Scoringsysteme, 2005, Bizer in Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. 2003, § 6a Rn. 12ff.

[267] Zu den telekommunikationsrechtlichen Fragen siehe: Müller, Ist das Auslesen von RFID-Tags zulässig? – Schutz von RFID-Transponderinformationen durch § 86 TKG, DuD, 2004, S. 215-217.

[268] Zur Funktionsweise von RFID in diesem Umfeld siehe Meyer: Wie RFID funktioniert – und wie nicht, CW, 25, 2005. Zu rechtlichen Problemstellungen auch Schaar, Datenschutzbeauftragter Peter Schaar warnt vor blauäugiger RFID-Nutzung, Interview in CW, 25/2005, S. 25.

store[269] bekannt geworden. Auch außerhalb dieses Umfeldes gibt es bereits Produkte, deren Verpackungen RFID enthalten (z.B. Gillette Rasierprodukte). Der Einsatz der RFID soll in diesen Fällen aber auf die Logistikkette begrenzt sein. RFID können in oder an einzelnen Produkten versteckt oder offen angebracht sein und den Einkaufs- wie auch den Bezahlvorgang steuern. Auch die schon beschriebenen Auswertungsvorgänge über das Kundeninteresse sind grundsätzlich möglich.

Ein Personenbezug des Kunden könnte über das Auslesen einer mit RFID versehenen Kundenkarte oder aber über das Zahlungsmittel vor dem Einkauf am Einkaufswagen oder erst mit seinem Abschluss an der Kasse hergestellt werden. Die eigentliche Auswertung des Kundenverhaltens findet in Hintergrundsystemen statt, auf die der Kunde keinen Einfluss hat. Er kann allenfalls durch den Verzicht auf eine Kundenkarte und die Verwendung anonymer Zahlungsmittel den Personenbezug verhindern.

Jedoch sind die Datenflüsse des Ubiquitous Computing für einen Kunden, der zunächst nur ein Geschäft betritt, nicht sichtbar. Relevant ist dabei insbesondere, dass eine Zuordnung des Produkt-Kunden mit dem Zahlungsmittel-Kunden stattfindet und dass eine Interessenauswertung über die zeitliche Aufenthaltsdauer in bestimmten Shopbereichen möglich ist. Das Ergebnis ist ein erheblicher Wissensüberschuss des Anbieters hinsichtlich der Interessen und Absichten seines Kunden, den er für eine zielgerichtete Kundenansprache nutzen kann.

3.4.2.2.2 Beispiel: Ticketing

Für die Fußball-Weltmeisterschaft 2006 in Deutschland wurde erstmals ein großflächiger Einsatz von RFID-Technik[270] in den Eintrittskarten für die Stadien geplant.[271] Da der Verkauf der Karten nur personalisiert erfolgte, sollte durch RFID-Leser an den Eingängen der Stadien und der verschiedenen Tribünen kontrolliert gesteuert werden, welche Personen sich an welchem Ort im Stadion aufhalten.[272] Mit einem derartigen Verfahren können Fans verschiedener Mannschaften getrennt, aber auch der Aufenthaltsort einzelner Personen zeitlich und räumlich eingegrenzt und nachverfolgt werden. Die Verknüpfung mit weiteren Mitteln, wie z.B. einer Videoüberwachung mit Gesichtserkennung, kann das Bewegungsprofil zur Totalüberwachung vervollständigen.

Neben einem orts- und zeitbezogenen Verhaltensprofil vor Ort kann über die Verbindung mit

---

[269] Zu im Kontext des Betriebes aufgetretenen Datenschutzproblemen siehe Tangens / Rosengart, BigBrotherAward 2003 – Verbraucherschutz, DANA, 04/2003, S. 8-10.

[270] Zu den weltweiten Anforderungen: Internationale Konferenz der Datenschutzbeauftragten: Entschließung zu Radio-Frequency Identification vom 20.11.2003, http://www.privacyconference2003.org/resolutions/RFIDResolutionGE.doc (27.03.2006).

[271] Deutscher Bundestag, Eintrittskarten zur Fußball-Weltmeisterschaft 2006 und Datenschutz (Kleine Anfrage), Bundestagsdrucksache 15/4896 vom 16.02.2005 und Antwort der Bundesregierung, Bundestagsdrucksache 15/5011 vom 07.03.2005.

[272] Weichert, Die Fußball-WM als Überwachungs-Großprojekt, DANA, 01/2005, S. 7-11; Conrad, RFID-Ticketing aus datenschutzrechtlicher Sicht, CR, 2005, S. 537ff., Holznagel / Bonnekoh, Radio Frequency Identification – Datenschutz v. Innovation?, MMR, 2006, S. 17 (21).

umfangreichen Registrierungsdatensätzen auch eine interessensbezogene Auswertung z.B. zu Werbezwecken vorgenommen werden.

Einflussmöglichkeiten der Karteninhaber auf das Ubiquitous Computing sind nicht vorhanden. Diese wollen mit der Inanspruchnahme ihrer Karte auch nicht aktiv und bewusst ihre personenbezogenen Daten preisgeben. Andererseits war der Kartenerwerb ohne Preisgabe personenbezogener Daten nicht möglich. Die RFID-Chips unbrauchbar zu machen, um eine Nachverfolgung zu unterbinden, hätte dem Betroffen jedoch die Nutzung der bereits bezahlten Leistung verwehrt, weil ohne eine Erkennung der auf dem Chip gespeicherten Informationen die RFID-Lesegeräte den Zugang zu dem Stadion nicht mehr freigeben sollten.

Die Verarbeitung und Auswertung der Daten erfolgte vollumfänglich in Hintergrundsystemen, zu denen der Betroffene keinen Zugang hat. Der Datenfluss ist nicht sichtbar. Lediglich die Anwesenheit von RFID-Lesegeräten könnte den Betroffenen auf eine Übertragung personenbezogener Daten schließen lassen. Die Informationen der RFID-Lesegeräte dürften in einem zentralen Hintergrundsystem zusammengelaufen sein und theoretisch eine Nachverfolgung von Personen mit bestimmten Tickets in Echtzeit ermöglicht haben. Aus dem Hintergrundsystem ließen sich dann Informationen auslesen wie bspw., dass sich Fan H im Fanblock einer Mannschaft befindet, die er nicht als Heimatteam angegeben hat, die nicht seiner Nationalität und auch nicht dem Land des Ticketerwerbs entspricht.

Im Nachgang zur Weltmeisterschaft teilte die Bundesregierung mit, dass eine Identitätskontrolle nie beabsichtigt gewesen sei. Das Sicherheitskonzept sei von einer stichprobenartigen Kontrolle ausgegangen. [273] Wie diese bei den VIP-Ticket-Kontingenten, die nicht personalisiert wurden, sondern nur den Sponsorennamen enthielten, stattfinden sollte, bleibt unklar.[274] Anders als das Organisationskommitte der Weltmeisterschaft, das das personalisierte Ticketing noch während der WM als sinnvoll erachtete,[275] hat sich die für die Fußball-Europameisterschaft 2008 zuständige UEFA bereits gegen eine Personalisierung der Eintrittskarten mittels RFID ausgesprochen.[276]

3.4.2.3 Umfeld: Haus/Wohnung

Die Wohnung dient seinen Bewohnern als Rückzugs- und Ruheraum.[277] Diese kann sie nur als überwachungsfreie Zone erfüllen. Ihre Schutzbedürftigkeit ist durch Art. 13 GG besonders anerkannt. Wer die Wohnung betreten darf, bestimmen ihre Bewohner. In der Regel

[273] Heise Newsticker, Bundesregierung: RFID-Chips für Masseneinsatz geeignet, http://www.heise.de/newsticker/meldung/75963 (19.07.2006).

[274] Heise Newsticker, Fußball-WM: Lückenlose Kontrolle gescheitert, http://www.heise.de/newsticker/meldung/74140 (12.06.2006).

[275] Heise Newsticker, Fußball-WM: OK hält personalisiertes Ticketing für sinnvoll, http://www.heise.de/newsticker/meldung/74917 (30.06.2006).

[276] Heise Newsticker, Fußball-WM: Zur EM wird alles anders, http://www.heise.de/newsticker/meldung/74448 (20.06.2006).

[277] Vgl. das Urteil zum großen Lauschangriff, BVerfG, 1 BvR 2378/98 vom 03.03.2004.

sind dies eingeladene Gäste oder Servicepersonal für bspw. Reparaturen oder Dienstleistungen.

Anwendungen des Ubiquitous Computing werden mit verschiedenen Zielrichtungen diskutiert.[278] Denkbar sind Sicherheitsmaßnahmen für den persönlichen Lebensbereich, der z.B. die Nachverfolgung von Personen und Gegenständen im gesamten Haus selbst beinhalten kann.[279] Weiterhin gelten so genannte Convenience-Anwendungen als wahrscheinlich, die den Komfort der Wohnung erhöhen und Wartungs- und Unterhaltungsarbeiten übernehmen. Einen weiteren Bereich wird das Feld hausinterner Kommunikation, aber auch der Kontakt der Bewohner zu Externen ausmachen. Letztlich sind auch Anwendungen im Unterhaltungsbereich denkbar.

Die Bewohner eines mit Ubiquitous Computing ausgestatteten Hauses können neben ihrer Rolle als Betroffene auch für die Verarbeitung der personenbezogenen Daten verantwortlich sein. Voraussetzung ist, dass sie Einfluss auf die Einstellung der Systeme nehmen können. Die technischen Funktionalitäten des Ubiquitous Computing könnten auch von einem externen Provider im Wege der Auftragsdatenverarbeitung (§ 11 BDSG)[280] übernommen werden. Diesem stünden damit möglicherweise hochsensible Daten der Bewohner zur Verfügung, deren Schutz und Verarbeitung präzise geregelt sein sollten. Als Betroffene sind darüber hinaus Dritte zu berücksichtigen, die entweder im Haus arbeiten (Servicepersonal) oder aber als Gäste für einen bestimmten Zeitraum die Einflusssphäre des Ubiquitous Computing betreten.

Von zu Hause aus handelt der Betroffene in einer Vielzahl von Rollen. So ist er möglicherweise Verbraucher und Empfänger von Telekommunikationsdienstleistungen oder Mediendiensten. Das Servicepersonal befindet sich in seiner Arbeitsumgebung. Gäste begeben sich in einen fremden Bereich, dem sie ähnlich viel Vertrauen entgegenbringen müssen wie ihrem eigenen persönlichen Lebensbereich.

Rechtliche Bestimmungsfaktoren für den Hausbereich ergeben sich aus dem Datenschutzrecht, da die Wohnung zentraler Raum für die Ausübung des allgemeinen Persönlichkeitsrechts ist, dem Verbraucherrecht, wenn die Bewohner ihren Konsumgewohnheiten von zu Hause aus nachgehen und Waren für den privaten Bedarf beschaffen, dem Telekommunikations- und Medienrecht bei der Nutzung von Kommunikationseinrichtungen nach außen aber auch hausintern (z.B. Funkverbindungen im Nahbereich), dem Umweltrecht, soweit Bestimmungen besondere Schutzstandards für den Einsatz von Technik im Bereich „home“ (z.B. Abstrahlung von Elektrogeräten) vorsehen und dem Arbeitsrecht, wenn Servicepersonal die Einflusssphäre der privaten Ubiquitous Computing-Anwendungen betritt (z.B. nur kurzzeitig: Postbote oder regelmäßig für längere Zeiträume: Reinigungspersonal, Babysitter). Daneben sind schließlich noch die Grundsätze des deliktischen Persönlichkeitsschutzes[281] zu beach-

[278] Siehe Kap. 2.

[279] Vgl. auch SWAMI: Scenario Analysis and Legal Framework – First Results, S. 6f.

[280] Siehe dazu auch die rechtliche Betrachtung zum zum Thema „Outsourcing“ (Kap. 6.2.1.2).

[281] Deutsch, Die neuere Entwicklung der Rechtsprechung zum Haftungsrecht, JZ, 2005, S. 987.

ten, soweit Dritte wie bspw. Gäste in den Einflussbereich häuslicher Ubiquitous Computing-Anwendungen kommen.

3.4.2.3.1 Beispiel: Licht- und Heizungssteuerung

Ein häufig genanntes Anwendungsbeispiel für die nähere Zukunft entstammt dem Convenience-Bereich.[282] Dabei sollen Einstellungen von Beleuchtungen oder der Heizung („An", „Aus", „Intensität") nach den Anwesenheiten oder Gewohnheiten bestimmter erkannter Benutzer automatisiert gesteuert werden.

Der Nutzer handelt dabei nicht unmittelbar (dies stellt gerade den Mehrwert dieser Form von Ubiquitous Computing dar), sondern die Aktion wird durch seine Anwesenheit und Identifizierung durch das Ubiquitous Computing-System ausgelöst. Seine Einflussnahme findet aber in der Regel vorher durch die Aktivierung und Konfiguration des Ubiquitous Computing-Systems nach seinen Wünschen statt. Etwas anderes könnte sich ergeben, wenn die Aktivierung z.B. in den Händen eines Vermieters oder eines Ubiquitous Computing-Providers liegt. Dann bliebe dem Betroffenen nur noch die Voreinstellung, die z.B. schon die Preisgabe bestimmter Preferenzdaten darstellt. Besucher oder Servicepersonal, die nur zu bestimmten Zeiten in den Räumen anwesend sind, werden in der Regel keinen Einfluss auf das Ubiquitous Computing-System nehmen können. Gleichwohl wird das System versuchen, solche Personen zunächst zu erkennen.

Hintergrundsysteme werden notwendig sein, um die Erkennung der Personen und ihre Preferenzen[283] vorzuhalten. Logdateien[284] solcher Systeme können die Bewegungen im Haus möglicherweise nachverfolgbar machen. Solche Nachverfolgungen können auf Grund einer begrenzten Anzahl von Personen im Haus zu bestimmten Zeiten leicht erfolgen und einer Person zugeordnet werden, selbst wenn diese dem System selbst nicht bekannt, weil nicht registriert ist.

Die Bewohner werden zumindest über die Funktionalitäten solcher Systeme informiert sein. Inwieweit auch die zugrunde liegende Datenverarbeitung transparent sein wird, ist nur schwer abzuschätzen. Für Externe (Gäste, Personal) ist ein solches Ubiquitous Computing-System zunächst nicht sichtbar.[285] Die Bewohner sind im Regelfall Betroffene. Zumindest der Inhaber der Wohnung bzw. des Hauses wird sich in einer Doppelrolle als Betroffener und als Verantwortlicher der personenbezogenen Datenverarbeitung befinden.

3.4.2.4 Umfeld: Kritische Infrastrukturen

Ein weiteres besonderes Anwendungsumfeld von Ubiquitous Computing-Systemen könnten kritische Infrastrukturen werden. Darunter können solche Einsatzbeispiele zusammengefasst

---

[282] Siehe Kap. 2.

[283] Zur Profilbildung siehe Roßnagel, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR, 2005, S. 71 (72).

[284] Schoen, Rechtliche Rahmenbedingungen zur Analyse von Log-Files, DuD, 2005, S. 84.

[285] Zur Kennzeichnungspflicht: Lahner, Anwendung des § 6 c BDSG auf RFID, DuD, 2004, S. 723.

werden, in denen von der einwandfreien Funktion vitale Interessen von Menschen oder Organisationen abhängen. Hier ist die Fehlertoleranz für technische Systeme wie für menschliches Verhalten besonders gering. Der Einsatz von Ubiquitous Computing-Systemen kommt besonders dann in Betracht, wenn technische Systeme so optimiert werden können, dass sie effektiver und mit größerer Fehlerfreiheit arbeiten als Menschen in der gleichen Situation. Dies sind bisher Situationen, in denen eine große Anzahl von Informationen in kurzer Zeit nach bestimmten Entscheidungsmustern abgearbeitet werden müssen. Solche Situationen treten meist in beruflichen Umfeldern auf, z.B. der Pilot eines Verkehrsflugzeugs, der Notarzt bei der Reanimation einer Person etc.

Auf Grund des besonderen Risikos der durch Ubiquitous Computing übernommenen Funktionalität werden hier vorwiegend haftungsrechtliche Bestimmungsfaktoren von besonderer Bedeutung sein. Da aber auch sehr sensitive Daten Betroffener einfließen können (z.B. Gesundheitsdaten), sind auch datenschutzrechtliche Normen als Bestimmungsfaktoren zu berücksichtigen. Da von Ubiquitous Computing-Systemen zur Unterstützung von kritischen Infrastrukturen zumeist Personen in ihrem beruflichen Umfeld betroffen sind, könnten auch arbeits- und berufsrechtliche Faktoren Einfluss auf ihre Entwicklung und Gestaltung haben.

3.4.2.4.1 Beispiel: Krankenhaus

In einem Krankenhaus sind eine Vielzahl von Ubiquitous Computing-Anwendungen denkbar, die einerseits der Automatisierung von Routineaufgaben dienen könnten (z.B. Blutdruck- und Fiebermessungen, Kontrolle von Medikamenteneinnahmen und Unverträglichkeiten) andererseits aber auch in kritischen Situationen Aufgaben übernehmen können (z.B. wenn ein Defibrilator die Reanimation einer Person anhand bestimmter Körpermerkmale automatisiert steuert). Dabei ist es den Anwendungen wesensimmanent, dass sie Entscheidungen und Handlungen für Dritte zu Gunsten der Betroffenen übernehmen sollen. Die Betroffenen befinden sich dabei häufig in der eingeschränkten Rolle als Patient ohne Einflussmöglichkeit auf die Ubiquitous Computing-Anwendung. Die Datenverarbeitung findet in Hintergrundsystemen statt, der Fluss personenbezogener Daten wird dem Patienten in der Regel nicht bewusst sein. Zudem wird es sich bei diesem Einsatzbeispiel häufig um Gesundheitsdaten und damit besonders sensitive Daten im Sinne von § 3 Abs. 9 BDSG handeln, die darüber hinaus besonderen Berufs- oder Amtsgeheimnissen unterliegen.

3.4.2.4.2 Beispiel: Flugzeug

Bereits Realität ist der Einsatz von Systemen im Cockpit von Airbusflugzeugen, die das Verhalten der Piloten verfolgen, kontrollieren und in bestimmten kritischen Situationen auch ändern. Ein Fehler in diesen Prozessen kann und hat bereits den Verlust von Menschenleben[286] zur Folge gehabt. Die Betroffenen wie bspw. die Piloten, das Personal sowie möglicherweise auch die Passagiere sind Gegenstand einer Verhaltenskontrolle. Der Einfluss der Betroffenen auf diese Ubiquitous Computing-Systeme ist begrenzt. Die Verarbeitung der Informationen findet in den Systemen des Flugzeugs statt, die über Flugschreiber und ähnli-

[286] Siehe Hilty, Vortrag auf dem 1. TAUCIS-Projektworkshop.

che Aufzeichnungsgeräte im Nachhinein nachvollzogen werden können. Der Datenfluss und die Entscheidungscharakteristik der Systeme dürften den Piloten zumindest in Teilen bekannt sein, den Passagieren hingegen kaum.

3.4.2.5 Kombination von Umfeldern

Eine besondere Problematik ergibt sich, wenn Ubiquitous Computing-Systeme über verschiedene Anwendungsumfelder hinweg arbeiten. Eine Typisierung in der zuvor beschriebenen Art lässt sich für die Kombinationen von Umfeldern nicht vornehmen, da diese einerseits sehr vielfältig sein können und andererseits gerade übergreifend sind, d.h. auch in verschiedene Situationen und Rollen einer Person hineinragen. Einige denkbare Probleme sollen daher anhand der nachfolgenden Beispielskombinationen aufgezeigt werden.

3.4.2.5.1 Beispiel: „Einkaufende“ Haushaltsgeräte

Im Rahmen des 1. TAUCIS-Projektworkshops wurde wiederholt das Beispiel der „einkaufenden“ Haushaltsgeräte zitiert. Dabei stellt ein Sensor im Glas eines Besuchers fest, dass das Glas sich leert. Dies stößt eine Aktion an, mit der überprüft wird, ob weitere Bestände des Getränks im Hause (z.B. im Kühlschrank) vorhanden sind. Wird dies verneint, so beginnt das Ubiquitous Computing-Gerät nach günstigen Anbietern zu suchen und ordert beim günstigsten Anbieter die zum Soll-Bestand fehlende Menge.

Dieses Beispiel ist anwendungsumfeldübergreifend im Hausumfeld/Convenience und im E-Commerce-Umfeld angesiedelt. Der Betroffene ist sowohl als Privatperson, möglicherweise auch als Arbeitgeber des Servicepersonals, aber auch als Verbraucher tätig. Eine ganze Reihe von Aktionen wird in dem Beispiel ausschließlich über Sensorik ausgelöst, ohne das der Betroffene eine bewusste Handlung in Richtung dieser Aktionen getätigt hätte. Seine Einflussmöglichkeiten auf ein solches System beschränken sich auf die Konfiguration des Systems, soweit er als Verantwortlicher einen Zugriff hat und über die entsprechende Kompetenz verfügt. Die Datenverarbeitung findet in Hintergrundsystemen verschiedener verantwortlicher Stellen statt und endet mit dem rechtsverbindlichen Abschluss eines Vertrages im Auftrag des Betroffenen.

Im Unterschied dazu ist der Betroffene (bzw. das von ihm eingesetzte System) in der Regel als Verbraucher tätig. Der tatsächliche Datenfluss dürfte nicht einmal dem Betroffenen (und Verantwortlichen) der Datenverarbeitung bewusst sein, da die Suche nach dem günstigsten Anbieter für eine bestimmte Ware eine Datenspur durch getätigte Anfragen hinterlässt und letztlich ein Vertrag mit einem Unternehmen geschlossen wird, welches der Betroffene konkret gar nicht kennt (da seine Ubiquitous Computing-Systeme über den Vertragspartner entschieden haben). Für die Rechnungskontrolle wird eine Protokollierung solcher angestoßener und durchgeführter Aktionen durch Ubiquitous Computing-Systeme unerlässlich sein.[287]

[287] Vgl. auch den Grundsatz der Revisionsfähigkeit als erforderliche technisch-organisatorische Maßnahme, Anhang zu § 9 BDSG.

3.4.3 Bestimmungsfaktoren

3.4.3.1 Informationelle Selbstbestimmung

Ubiquitous Computing-Systeme erfassen Kontextinformationen, die dann einer bestimmten oder bestimmbaren Person zugeordnet werden können. Solche Informationen tangieren das informationelle Selbstbestimmungsrecht des Betroffenen und sind damit relevant im Sinne von Art. 2 Abs. 1 in Verbindung von Art. 1 Abs. 1 des Grundgesetzes (GG) und § 1 des Bundesdatenschutzgesetzes (BDSG).

3.4.3.1.1 Rechtsrahmen

Das informationelle Selbstbestimmungsrecht ist spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts[288] als Teil des allgemeinen Persönlichkeitsrechts und damit als Grundrecht anerkannt.[289] Es ist ebenfalls in Art. 8 der Europäischen Menschenrechtskonvention (EMRK) und im Verfassungsentwurf der Europäischen Union verankert. Es ermöglicht allen natürlichen Personen, selbst frei über die Verwendung von Informationen zu entscheiden, die sie selbst betreffen oder einen Bezug zu ihnen aufweisen. Auf diese Weise soll verhindert werden, dass Personen zum Spielball Dritter (dies können öffentliche oder private Stellen, z.B. Unternehmen sein) werden, die durch die Sammlung und Auswertung personenbezogener Daten einen Informationsüberschuss gegen den Willen des Betroffenen ausnutzen könnten.

Das informationelle Selbstbestimmungsrecht ist durch eine Vielzahl von Regelungen auf einfachgesetzlicher Ebene konkretisiert. Den Kernbereich allgemeiner Regelungen stellen dabei das Bundesdatenschutzgesetz sowie die Landesdatenschutzgesetze dar. Letztere gelten für personenbezogene Datenverarbeitungen der öffentlichen Stellen der jeweiligen Länder. Das BDSG regelt die Verarbeitungen der öffentlichen Stellen des Bundes und der sogenannten nicht-öffentlichen Stellen, also z.B. Unternehmen, Vereine oder Privatpersonen. Eine Vielzahl weiterer Regelungen findet sich in bereichsspezifischen Gesetzen wie z.B. dem Teledienstedatenschutzgesetz (TDDSG), dem Telekommunikationsgesetz (TDG)[290] oder dem Sozialgesetzbuch. Diese Regelungen werden maßgeblich durch europäische Vorgaben, insbesondere die EG-Datenschutzrichtlinie[291] und die EG-Datenschutzrichtlinie für elektronische Kommunikation[292] beeinflusst, die europaweite Datenschutzmindeststandards etablieren.

Allen Regelungen gemein ist ein Kanon von Grundprinzipien, die die legale Verarbeitung

[288] BVerfGE 65, S. 1.

[289] Zum informationellen Selbstbestimmungsrecht: Gola / Schomerus, BDSG, § 1 Rn. 9.

[290] Ohlenburg, Der neue Telekommunikationsdatenschutz, MMR, 2004 S. 431ff.

[291] Richtlinie 95/46/EG.

[292] Richtlinie 2002/58/EG.

unterschiedlichster personenbezogener Daten[293] bestimmen. Für die Zulässigkeit einer personenbezogenen Datenverarbeitung gilt der sogenannte *Verbotstatbestand mit Erlaubnisvorbehalt* wie er beispielsweise in § 4 Abs. 1 BDSG, § 3 Abs. 1 TDDSG, § 17 Abs. 1 Mediendienste-Staatsvertrag (MDStV) zu finden ist. Danach sind personenbezogene Datenverarbeitungen nur erlaubt, wenn die Einwilligung des Betroffen der Verarbeitung vorliegt oder aber eine Rechtsvorschrift die Verarbeitung erlaubt oder anordnet. Dies führt in der Praxis dazu, dass für jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Zusammenhang mit Ubiquitous Computing entweder die Einwilligung des Nutzers oder aber eine Rechtsvorschrift vorliegen muss, die die Verarbeitung erlaubt.

Eine *Einwilligung* des Betroffenen muss dabei auf informierter Basis erfolgen (vgl. § 4 Abs. 3, § 4a Abs. 1 S. 2 BDSG, § 4 Abs. 3 TDDSG), das heißt der von Ubiquitous Computing Betroffene muss beispielsweise darüber informiert werden, für welche konkreten Zwecke die personenbezogenen Daten in der Folge verwandt werden und dass ein Widerruf mit Wirkung für die Zukunft möglich ist. Weiterhin muss die Einwilligung eine freie Entscheidung des Betroffenen über seine Daten zum Ausdruck bringen (vgl. § 4a Abs. 1 S. 1 BDSG).

Formell verlangt das Gesetz im Offline-Bereich aus Beweisgründen und als Übereilungsschutz in der Regel die *Schriftlichkeit einer Einwilligung* (vgl. § 4a Abs. 1 S. 3 BDSG). Da Schriftform ersetzende Signaturen (nach Signaturgesetz, vgl. auch § 126 Abs. 3, § 126a, § 126b Bürgerliches Gesetzbuch (BGB)) bisher keine praktische Verbreitung gefunden haben, sieht das Teledienstedatenschutzgesetz für den Fall einer elektronischen Einwilligung eigene Anforderungen für eine wirksame Einwilligung vor (§ 4 Abs. 2 TDDSG). Neben der Einwilligung kommen verschiedene Rechtsvorschriften als Erlaubnistatbestände in Betracht, die eigene Tatbestandsvoraussetzungen enthalten und häufig eine Abwägung des Interesses des Betroffenen an der Erhaltung seiner Privatsphäre und der berechtigten Interessen der verantwortlichen Stelle an einer Verarbeitung der personenbezogenen Daten erfordern.

Bei einer Verarbeitung auf Grund einer gesetzlichen Erlaubnisnorm verlangt das Datenschutzrecht die *Erforderlichkeit* der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Dies beinhaltet, dass die Art und der Umfang der personenbezogenen Daten geeignet und notwendig sind, um den Zweck der Datenverarbeitung zu erfüllen. Zudem sollen personenbezogene Daten in möglichst geringem Umfang verarbeitet werden. Als für die Gestaltung von Ubiquitous Computing-Systemen besonders wichtige Ausprägung dieses Grundprinzips ist der Grundsatz der *datenvermeidenden und datensparsamen Gestaltung* von Datenverarbeitungssystemen anzusehen (vgl. § 3a S. 1 BDSG).[294] Darüber hinaus soll auch von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch gemacht werden, wo dies mit angemessenem Aufwand möglich ist (§ 3a S. 2 BDSG). Dies gilt insbesondere auch für die Inanspruchnahme von Telediensten also z.B. des Internets durch

[293] Zur Definition personenbezogener Daten siehe § 3 Abs. 1 BDSG und Saeltzer, Sind diese Daten personenbezogen oder nicht? DuD, 2004, S. 218ff.

[294] Zur Datensparsamkeit bei RFID siehe Müller/Handy, RFID und Datenschutzrecht, DuD, 2004, S. 655 (657). Danach sind RFID-Tags als potentieller Gegenstand einer Datenverarbeitung zu deaktivieren oder zu entfernen.

den Nutzer (vgl. § 4 a Abs. 6 TDDSG). Ebenfalls Bestandteil des Grundsatzes der Erforderlichkeit ist die Einhaltung von Sperr- und Löschfristen nach dem Wegfall einer Verarbeitungs- oder Nutzungserlaubnis (vgl. § 35 Abs. 2, 3 und 8 BDSG).

In enger Verbindung zu der Erforderlichkeit steht der allgemeine *Zweckbindungsgrundsatz*. Danach dürfen personenbezogene Daten nur zu vorher konkret festgelegten Zwecken (Primärzweck) erhoben, verarbeitet oder genutzt werden (vgl. § 28 Abs. 1 S. 2 BDSG).[295] Zweckänderungen sind grundsätzlich möglich, sie bedürfen jedoch einer dem neuen Zweck entsprechenden Rechtsgrundlage (Einwilligung oder Rechtsvorschrift, vgl. § 28 Abs. 3, § 3 Abs. 2 TDDSG) und lösen zusätzliche Informationspflichten aus (§ 4 Abs. 3, § 28 Abs. 4 S. 2 BDSG). Im Sonderfall der Zweckänderung zur Nutzung für Werbezwecke steht dem Betroffenen ein Widerspruchsrecht zu, auf das er hinzuweisen ist (§ 28 Abs. 4 S. 2 BDSG). Die Einhaltung der Zweckbindung ist durch technisch-organisatorische Maßnahmen (§ 9 BDSG) abzusichern. Der Verwendung von in anderen Zusammenhängen gesammelten personenbezogenen Daten zur Bildung von Nutzungsprofilen an digitalen Inhalten steht der Grundsatz der Zweckbindung entgegen. Eine solche Profilbildung über Nutzungsverhalten erfordert eine informierte, freiwillige Einwilligung des Betroffenen für alle einfließenden Daten. Eine gesetzliche Grundlage, insbesondere § 28 Abs. 1 Nr. 2 BDSG, vermag eine solche Nutzung nicht zu legitimieren.

Der datenschutzrechtliche Grundsatz der *Transparenz* personenbezogener Datenverarbeitung legt das notwendige Wissensfundament für eine Ausübung des informationellen Selbstbestimmungsrechts durch den Betroffenen. Ohne Information darüber, welche Erhebungen, Verarbeitungen oder Nutzungen seiner personenbezogenen Daten geplant sind oder gerade stattfinden, kann er nicht effektiv darüber entscheiden, ob er eine solche Verarbeitung wünscht oder Maßnahmen dagegen treffen muss. Als gesetzliche Ausprägung des Transparenzgrundsatzes sieht das Datenschutzrecht vielfältige Unterrichtungs- und Informationspflichten der verantwortlichen Stelle (vgl. als Beispiel § 4 Abs. 3, § 33 Abs. 1 BDSG, § 4 Abs. 1 TDDSG) vor.[296] Hierzu zählen außerdem die bereits genannte Informationspflicht im Kontext einer Einwilligung (§ 4a Abs. 1 BDSG) und die Hinweispflicht auf ein Widerspruchsrecht (z.B. § 28 Abs. 4 S. 2 BDSG). Darüber hinaus steht dem Betroffenen ein Auskunftsanspruch über gespeicherte personenbezogene Daten, deren Herkunft, eventuelle Empfänger oder Empfängerkategorien und den Zweck der Verarbeitung zu (§ 34 Abs. 1 BDSG). Ebenfalls zur Transparenz der Datenverarbeitung soll der Regelfall der Direkterhebung personenbezogener Daten beim Betroffenen beitragen. Danach sind personenbezogene Daten beim Betroffenen zu erheben, soweit nicht eine Rechtsvorschrift etwas anderes vorsieht oder der Geschäftszweck eine Dritterhebung erforderlich macht oder die Direkterhebung einen unverhältnismäßig hohen Aufwand erfordern würde (§ 4 Abs. 2 S. 2 BDSG). In diesen Ausnahmefällen ist jedoch noch eine Interessenabwägung dahin gehend vorzunehmen, dass keine

[295] Zur Zweckbindung beim UC siehe Roßnagel / Müller, Ubiquitous Computing, Neue Herausforderungen für den Datenschutz, CR, 2004, S. 625 (630).

[296] Zur Transparenz beim UC vgl. insb. Roßnagel / Müller, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR, 2004, S. 625 (629ff.).

Anhaltspunkte für die Beeinträchtigung überwiegend schutzwürdiger Interessen des Betroffenen bestehen.

Weiterhin muss für den Bestand an personenbezogenen Daten, die von einer verantwortlichen Stelle vorgehalten werden, sichergestellt werden, dass die Daten auch inhaltlich korrekt sind (*Qualität* der Daten). Bei einer Verwendung der Daten für eigene Geschäftszwecke wird die verantwortliche Stelle daran bereits ein Eigeninteresse haben. Erfolgen Datensammlungen jedoch zur Weiterveräußerung, ist dies nicht immer gegeben. In jedem Fall können falsche personenbezogene Daten rechtliche und andere nachhaltige negative Folgen für den Betroffenen haben. Daher steht dem Betroffenen als Ergänzung des bereits erwähnten Auskunftsanspruchs ein Berichtigungsanspruch für seine personenbezogenen Daten gegen die verantwortliche Stelle zu (§ 35 Abs. 1 BDSG). Für die Zeit zwischen Geltendmachung dieses Anspruchs und der tatsächlichen Berichtigung dürfen die umstrittenen Daten nicht verarbeitet oder genutzt werden (§ 35 Abs. 4, 6, 7). In Ergänzung des Berichtigungsanspruchs besteht die Verpflichtung der verantwortlichen Stelle, etwaige Empfänger falscher personenbezogener Daten über diesen Umstand in Kenntnis zu setzen (§ 35 Abs. 7 BDSG).

Der Schutz personenbezogener Daten, die automatisiert in Datenverarbeitungsanlagen verarbeitet werden, lässt sich generell nur gewährleisten, wenn die verantwortliche Stelle die vollständige und alleinige Verfügungsgewalt über die Datenverarbeitungsanlage ausüben kann. Der *Grundsatz der Sicherheit* personenbezogener Daten ist daher nur sicherzustellen, wenn ein dem Risiko angemessenes Maß an IT-Sicherheit bereitgestellt ist. Dazu gehören hinreichende Verschlüsselungsmaßnahmen bei der Übertragung personenbezogener Daten ebenso wie ihre sichere, gegen Zugriff unbefugter Dritter geschützte Verwahrung. Aufgrund der Vielfältigkeit personenbezogener Datenverarbeitungssysteme beschränkt sich das Gesetz auf die recht allgemein gehaltene Verpflichtung, dass die verantwortliche Stelle die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen hat, um die Ausführung der gesetzlichen Anforderungen zu gewährleisten (§ 9 BDSG). Ein genaueres Prüfungsraster für den Einzelfall hält die Anlage zu § 9 BDSG bereit. Darin ist als Bestandteil des Grundsatzes der Datensicherheit u.a. die Revisionsfähigkeit personenbezogener Datenverarbeitung verankert. Danach müssen einzelne Verarbeitungsvorgänge nachvollziehbar dokumentiert werden.

Wendet man diese Grundsätze in ihren jeweiligen gesetzlichen Ausformungen auf die geschilderten Beispiele an, so ergeben sich Problemfelder, in denen sich die Anwendungen des Ubiquitous Computing nicht oder nur mit zusätzlichem Aufwand mit datenschutzrechtlichen Regelungen vereinbaren lassen.[297] Eine fehlende Rechtskonformität, wie auch die daraus möglicherweise resultierende fehlende Akzeptanz der Technik beim Nutzer, kann sich als bestimmender rechtlicher Faktor für Ubiquitous Computing im jeweils genannten Anwendungsumfeld erweisen. Die nachfolgenden rechtlichen Bestimmungsfaktoren ergeben sich für den Bereich des informationellen Selbstbestimmungsrechts:

[297] Vgl. Roßnagel / Müller, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR, 2004, S. 625ff.

3.4.3.1.2 Überwachungsdruck

Die von den Sensoren einer Ubiquitous Computing-Umgebung erfassten Informationen liegen digital und damit in Formaten vor, die automatisiert weiterverarbeitet und ausgewertet werden können. Kontextverknüpfungen und Schnittstellen sind integraler Bestandteil der Ubiquitous Computing-Systeme. Dies eröffnet sehr umfassende Überwachungsmöglichkeiten für eine Vielzahl von Systemen, in der Produktions- und Logistiksteuerung ebenso wie in der Auswertung und Weiterverarbeitung von Shopinformationen oder der Überwachungsdaten in Stadien.

Solche Informationsflüsse sind für die Betroffen durchweg nicht transparent. Eigene Einflussmöglichkeiten sind für den Nutzer regelmäßig nur durch gänzlichen Verzicht auf die Anwesenheit im Anwendungsumfeld gegeben. Dies würde in bestimmten Fallgestaltungen die Aufgabe des Arbeitsplatzes[298] oder den Verzicht auf den Besuch öffentlicher Veranstaltungen bedeuten. Realistisch betrachtet wird der Betroffene in vielen Fällen sein allgemeines Persönlichkeitsrecht zurückstellen, um nicht finanzielle oder gesellschaftliche Nachteile in Kauf nehmen zu müssen. Die Einführung von Ubiquitous Computing in bestimmten Kontexten kann den Bürger damit in die Zwangslage bringen, zwischen zwei möglicherweise gravierenden Übeln wählen zu müssen. Eine Vielzahl solcher erzwungener Entscheidungen durch die flächendeckende Einführung von Ubiquitous Computing könnte dann zu einem Gefühl der Unfreiheit führen.

Wird eine strenge Bindung der konkreten Anwendung an den dem Nutzer bekannten Zweck nicht eingehalten, so wird der Betroffene an unterschiedlichen Stellen oder auch mit großen Zeitabständen mit seinen personenbezogenen Daten oder der Auswertung seiner Person konfrontiert werden, wo er dies nicht (mehr) erwartet. Eine „Grundtradition des Vergessens“ wie sie heute gesellschaftlich gewollt und gesetzlich implementiert (z.B. Löschung von Verkehrsverstößen im Flensburger Bundeszentralregister, Löschung von Einträgen im Bundeszentralregister) ist, könnte damit unmöglich werden. Mit einer solchen zeitlich und inhaltlich nahezu unbegrenzten Verantwortlichkeit für eigene Datenspuren wächst das Gefühl der Menschen, der Technik ausgeliefert zu sein und permanent kontrolliert zu werden.

Das Gefühl permanenter Kontrolle kann zu Verhaltensänderungen des Beobachteten führen, mit der Folge, dass dieser sich in der Beobachtungssituation nicht entsprechend seines freien Willens sondern nach vermuteten Erwartungshaltungen verhalten wird. Das Datenschutzrecht hat die Aufgabe, einer solchen Entwicklung zu begegnen.[299]

Auf einfachgesetzlicher Ebene versuchen insbesondere die vielfältigen Transparenzpflichten „einem dumpfen Gefühl“ des Überwachtwerdens entgegenzuwirken, indem eine Überwachung klar kenntlich gemacht werden muss. Eine der Überwachung mittels Ubiquitous Computing-Systemen ähnliche Situation ergibt sich schon jetzt bei der Videoüberwachung, die zumindest in deutschen Innenstädten ob ihres gehäuften Auftretens bereits heute

[298] Zur Zulässigkeit der Überwachung am Arbeitsplatz vgl. Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, S. 433ff.

[299] Vgl. die instruktiven Anmerkungen im Volkszählungsurteil, BVerfGE 65, 1.

als „allgegenwärtig“ betrachtet werden kann. Für diese Fälle besteht eine Kennzeichnungspflicht der Videoüberwachungsanlagen an öffentlich zugänglichen Orten gem. § 6 b BDSG. Die Videoüberwachung in deutschen Innenstädten wird von einer Vielzahl verantwortlicher Stellen vorgenommen. Dies hat zu Folge, dass die erhobenen Datenbestände in der Regel nicht in einem System zugänglich und damit ein großer Datenbestand zentralisiert automatisiert auswertbar ist. Dieser Umstand mag das Überwachungsgefühl möglicherweise reduzieren. Für die Entwicklung des Ubiquitous Computing wird es daher wichtig sein, ob das Gefühl der Überwachung durch eine Transparenzpflicht sowie durch eine Isolierung einzelner Systeme reduziert werden kann.

Die Anforderungen des informationellen Selbstbestimmungsrechts zur Verhinderung eines übermäßigen Überwachungsdrucks stehen einer Entwicklung des Ubiquitous Computing nicht entgegen, wohl aber einer Verarbeitung, die mit den Grundsätzen der informationellen Selbstbestimmung nicht übereinstimmen. Der Datenschutz wird also eine Entwicklung bremsen, in der Ubiquitous Computing den Überwachungsdruck auf die Menschen erhöht. Ein solcher Effekt wird allerdings nicht für Ubiquitous Computing-Systeme zu erwarten sein, die die informationelle Selbstbestimmung des Nutzers angemessen berücksichtigen. Eine Beurteilung dessen, was z.B. im Hinblick auf Transparenzanforderungen[300] angemessen ist, wird jedoch für jedes einzelne Anwendungsumfeld und die dort eingesetzten Ubiquitous Computing-Systeme zu beurteilen sein. Entscheidend ist letztlich, ob der Kreis der Betroffenen eingegrenzt, die Transparenz an ihren Bedürfnissen orientiert und mit Entscheidungsmöglichkeiten gestaltet werden kann.

3.4.3.1.3 Profilbildung und -auswertung

In vielen Beispielen beruht die Funktionalität des Ubiquitous Computing auf der Vernetzung von Sensoren mit Hintergrunddatenbanken (Kontexten), auf deren Grundlage die Objekte an der Person orientierte Aktionen auslösen.

Dabei können für den Betroffenen nachteilige Entscheidungen automatisiert ohne Einschaltung eines Menschen getroffen werden. Solche Fälle werden datenschutzrechtlich bisher vorwiegend im Bereich des so genannten Scorings diskutiert. Beim Scoring wird die Wahrscheinlichkeit eines zukünftigen Verhaltens einer Person durch eine statistisch mathematische Analyse von Vergleichsdaten ermittelt.[301] Solche Systeme arbeiten nicht mit künstlicher Intelligenz oder genetischen Algorithmen, wie dies für Ubiquitous Computing-Systeme diskutiert wird, sondern basieren „nur“ auf einem vergleichsweise einfachen festgelegten Verfahrensablauf und Kriterienraster. Vergleichbar mit dem Ubiquitous Computing ist aus Betroffenensicht, dass personenbezogene Daten in elektronischer Form zur weiteren automatisierten Auswertung vorliegen und dass weitere Verarbeitungsschritte vorgenommen werden, die für den Betroffenen zunächst nicht sichtbar sind, aber zu einem spürbaren Ergebnis führen.

---

[300] Zur Transparenz beim UC siehe Roßnagel / Müller, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR 2004, S. 625 (629ff.).

[301] Möller / Florax, Kreditwirtschaftliche Scoring-Verfahren, MMR, 2002, S. 806; ULD, Scoringsysteme 2005.

Für solche Fälle einer automatisierten Einzelentscheidung sieht das BDSG in § 6 a besondere Zulässigkeitsvoraussetzungen vor, die auf die entscheidungsnotwendige Transparenz und eine Einflussnahme- bzw. Korrekturmöglichkeit des Betroffenen einer negativen automatisierten Einzelentscheidung abzielen. Diese Norm könnte auch den Einsatz von Ubiquitous Computing-Systemen besonderen Anforderungen unterwerfen, soweit die Verarbeitung zur Bewertung einzelner Persönlichkeitsmerkmale erfolgt. Die Verweigerung des Zutritts einer Person zu WM-Stadien mittels RFID-Ticket und einer ausschließlich automatisierten Auswertung von im Hintergrundsystem hinterlegten personenbezogenen Daten (z.B. „Straffällig geworden wegen Sachbeschädigung in Stadien“) dürfte danach einen Verstoß gegen § 6 a BDSG darstellen, soweit solche Prüfungen gegenüber dem Betroffenen nicht transparent gemacht werden und ihm keine wirksame Möglichkeit zur Klarstellung/Berichtigung eingeräumt wird.

Für viele Auswertungen personenbezogener Datenbestände, wie sie in Hintergrundsystemen auflaufen, ist die informierte Einwilligung des Nutzers nach § 4 a BDSG (bzw. gem. § 4 TDDSG, soweit es sich um einen Teledienst gem. § 2 Abs. 1 TDG handelt) erforderlich, da Rechtsnormen keinen einschlägigen Erlaubnistatbestand enthalten.[302]

Zwar können Ubiquitous Computing-Systeme zur Vertragserfüllung eingesetzt werden, so dass gem. § 28 Abs. 1 S. 1 BDSG eine Erlaubnisnorm vorläge, doch sind Profile und deren Auswertung meist nicht zur Erfüllung einer Vertragsbeziehung erforderlich, sondern zielen vielmehr auf den Abschluss neuer Verträge, also auf Werbung oder Markt- und Meinungsforschung ab (z.B. die Auswertung der Kundeninteressen im Shopbeispiel). Dies stellt einen alternativen Zweck oder eine Zweckänderung dar, die einer neuen eigenständigen Rechtsgrundlage bedürfte (vgl. § 28 Abs. 3 BDSG). § 28 Abs. 1 S. 1 Nr. 2 BDSG wird hier nicht in Betracht kommen, da die Interessensabwägung beim Profiling in der Regel zu Gunsten des Rechts des Betroffenen ausfällt.[303]

Datenschutzrechtliche Anforderungen im Hinblick auf die Profilbildung werden die Implementierung des Ubiquitous Computing in Anwendungen nicht beschränken, wohl aber den Funktionsumfang der Hintergrundsysteme. Ob die mit Ubiquitous Computing angestrebten Rationalisierungs- und Synergieeffekte mit einer solchen Beschränkung erreicht werden können, lässt sich nicht abschätzen. Möglicherweise eröffnen hier Konzepte der Pseudonymisierung oder Anonymisierung der Datenbestände neue Möglichkeiten.

3.4.3.1.4 Transparenz

Die Datenverarbeitung in Ubiquitous Computing-Systemen ist wegen ihrer technischen Ausgestaltung und der Kontextverknüpfungen sehr komplex. Bei einer personenbezogenen Datenverarbeitung ist jedoch eine hinreichende Information der Betroffenen über ihre Erfassung

[302] Zur angepassten Nutzung der Einwilligung im UC siehe Rossnagel / Müller, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR, 2004, S. 625 (629).

[303] Zum Profiling: Roßnagel, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR, 2005, S. 71 (72); Langheinrich, Die Privatspäre im Ubiquitous Computing, http://www.vs.inf.eth.ch/publ/papers/langhein2004rfid.pdf (04.02.2006).

(z.B. durch ein akustisches oder optisches Signal) sowie die Zwecke der Verarbeitung (durch Text, Bild oder Ton)[304] erforderlich, soweit ihnen diese nicht schon bekannt sind.

Das Datenschutzrecht hat mit dem in der letzten Novellierung neu geschaffenen § 6 c BDSG eine erste Regelung zur Transparenz der personenbezogenen Datenverarbeitung bei „mobilen personenbezogenen Speicher- und Verarbeitungsmedien“ erhalten. Danach besteht eine Informationspflicht der verantwortlichen Stelle, die solche Medien ausgibt oder Verfahren, die auch nur teilweise auf einem solchen Medium ablaufen, auf diesem Medium aufbringt, ändert oder hierzu bereithält. Der Betroffene ist dabei über die Identität und die Anschrift der verantwortlichen Stelle, die Funktionsweise der Technik, die Art der zu verarbeitenden personenbezogenen Daten, die Möglichkeit der Ausübung von Auskunfts-, Berichtigungs- und Löschrechten und die Maßnahmen bei Verlust oder Zerstörung des Mediums zu informieren. Darüber hinaus müssen Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen für den Betroffenen eindeutig erkennbar sein. Die Geltung dieser Vorschrift bezieht sich nicht auf Chips, die ausschließlich ausgelesen werden können (da keine Verarbeitung auf dem Chip erfolgt), sie findet aber z.B bei der Übermittlung personenbezogener Daten durch aktive RFID-Chips Anwendung.[305]

Eine Kenntnis des Betroffenen wird man in der Regel für einen sehr globalen und damit noch unbestimmten Primärzweck der meisten Ubiquitous Computing-Anwendungen annehmen können. Konkrete Zwecke (z.B. die Verwendung zur Profilbildung zu Werbezwecken in den Hintergrundsystemen) werden gegenüber den Betroffenen gesondert kenntlich zu machen sein. Art und Ort einer solchen Information werfen Darstellungsprobleme auf, soweit der Nutzer lediglich in den Anwendungsbereich eines Ubiquitous Computing-Systems kommt, zu dessen Nutzung er keinerlei Vereinbarungen getroffen hat. Die Informationsprobleme in diesen Fällen potenzieren sich, wenn mehrere Ubiquitous Computing-Systeme parallel im Einsatz sind. Möglicherweise wird sich ein Teil dieses Problems durch eine besonders umfassende Information des Nutzers vor dem (erstmaligen) Einsatz der Ubiquitous Computing-Anwendung lösen lassen. Dies entspräche zumindest in zeitlicher Hinsicht der derzeitigen gesetzlichen Regelung für den Einsatz von Cookies im WWW zur personenbezogenen Datenverarbeitung (vgl. § 4 Abs. 1 TDDSG) und auch der in § 6 c BDSG geforderten Information („zu verarbeitenden Daten“).

Wichtig ist die Information der Betroffenen nicht nur zur Erfüllung datenschutzrechtlicher Vorgaben, sondern auch für die Akzeptanz der jeweiligen Ubiquitous Computing-Anwendung. Eine effektive Umsetzung der Erfüllung der Transparenzanforderung wird die Entwicklung von Ubiquitous Computing befördern, wenn der Betroffene seine individuellen Nutzen und Kosten einer solchen Verarbeitung erkennen und bewerten kann und zu einem

[304] Hier sind technische Möglichkeiten wie sie z.B. die P3P-Plattform bietet von besonderer Bedeutung, so auch Rossnagel / Müller, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR, 2004, S. 625 (629), Roßnagel, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR, 2005, S. 71 (74).

[305] Bizer in: Simitis, BDSG, 5. Aufl, § 3, Rn. 277; Gola / Schomerus, BDSG, § 6 c Rn. 2, Kelter/Widmann, Radio Frequency Identification, DuD, 2004, 331.

positiven Ergebnis kommt. Zu beachten ist, dass sich eine Umsetzung der Transparenzanforderung, die die Nutzungsfreundlichkeit der Anwendung beeinträchtigt, negativ auf die Informationswirkung (vgl. „Wegklicken“ von Warnhinweisen im Browser) wie auch die Akzeptanz der Anwendung selbst niederschlagen kann.

3.4.3.1.5 Bereichsspezifische Regelungen

Besonders sensible personenbezogene Daten nach § 3 Abs. 9 BDSG oder solche, die in besonderen Beratungs-, Behandlungs- oder Betreuungsverhältnissen anfallen, unterliegen besonderen Schutzanforderungen. Verstöße gegen Berufs- oder Amtsgeheimnisse z.B. der Rechtsanwälte oder Ärzte und ihres Personals sind nach § 203 Strafgesetzbuch (StGB) strafbewehrt. Solche besonderen Schutzmechanismen können im Ubiquitous Computing-Beispiel der automatisierten Reanimation aber auch in wesentlich einfacheren Gestaltungen zum Tragen kommen, wenn z.B. eine automatisierte Terminverwaltung Arzt-, Anwaltstermine mit Patienten oder Mandanten offenbart. Eine Offenbarung von durch Berufs- oder Amtsgeheimnissen geschützten Daten an Dritte (z.B. Ubiquitous Computing-Provider) ist jedoch ohne Einwilligung des Betroffenen grundsätzlich unzulässig.

3.4.3.1.6 IT-Sicherheit

Werden in Ubiquitous Computing-Systemen oder deren Komponenten personenbezogene Daten (z.B. über Funk) übertragen, so sind diese gegen einen Zugriff Dritter zu schützen. Entsprechendes gilt für den Schutz personenbezogener Daten in den Hintergrundsystemen. Dies ergibt sich aus § 9 BDSG, der die Umsetzung „der erforderlichen technischen oder organisatorischen Maßnahmen für den Schutz personenbezogener Daten“ von der verantwortlichen Stelle fordert.

Die Bestimmung der für die personenbezogene Datenverarbeitung verantwortlichen Stelle könnte sich als Problemfeld des Ubiquitous Computing erweisen.[306] Die Bestimmung dieser Stelle ist zentral für die Geltendmachung verschiedener Betroffenenrechte, die die Basis der notwendigen Information enthalten. Die Anknüpfung des Datenschutzrechts an diesen Begriff ging von der technischen Datenverarbeitung in den 70er Jahren aus. Damals verantwortete eine zentrale Stelle die Datenverarbeitung, die sie in großen Rechenzentren vornehmen ließ. Eine solche Situation ist beim Ubiquitous Computing strukturell nicht mehr vorhanden, da hier eine Vielzahl von Personen sowohl Betroffener als auch Verantwortlicher von personenbezogener Datenverarbeitung sein wird.[307]

Zwar wird der Einsatz des Ubiquitous Computing auch durch jemanden initiiert und betrieben werden, der ein Interesse an der mit dem Ubiquitous Computing beabsichtigten Zweckerreichung hat (dies kann z.B. ein geschäftliches, aber auch ein privates Interesse wie im Convenience-Beispiel sein). Doch wird vielen solcher „verantwortlichen Stellen“ nur noch der Betrieb der Funktionalität mit Mitteln des Ubiquitous Computing, nicht aber die damit verbundene Datenverarbeitung bewusst und verständlich sein. So wird sich die Privatperson, die eine

[306] Vgl. auch Garstka, Protokoll zum 1. TAUCIS Workshop.

[307] Vgl. Rossnagel, Pfitzmann, Garstka, Modernisierung des Datenschutzrechts, S. 22ff., 185f.

selbstregulierende Heizungsanlage betreibt, wohl regelmäßig nicht darüber bewusst sein, dass sie Anwesenheits- und Bewegungsprofile ihrer Hausbewohner oder Gäste in bestimmten Räumen erfasst, speichert und auch auswertet. Angenommen das Datenschutzgesetz käme im Fall der privaten Heizungsanlagen nicht zur Anwendung, weil und soweit die Datenerhebung, -verarbeitung und -nutzung „ausschließlich für persönliche oder familiäre Tätigkeiten“ im Sinne von § 27 Abs. 1 S. 2 BDSG erfolgt, dann könnte der ohne Wissen und Vorsatz handelnde Betreiber einer solchen Anlage von dem Geschädigten nur im Rahmen der Verletzung von Sorgfaltspflichten zur Verantwortung gezogen werden.[308] Selbst wenn sich die Betreiber gegen solche Folgen versichern könnten, so würden über eine solche Haftungslösung Schäden allenfalls kompensiert, aber nicht verhindert werden. Angenommen das Datenschutzgesetz findet auf den erfassten Gast Anwendung, dann wird der Privatanwender darauf angewiesen sein, dass ihn die Anlage standardmäßig unterstützt, die Datenschutzrechte Dritter zu wahren und nicht zu beeinträchtigen.

Privatanwender werden regelmäßig nicht in der Lage sein, die erforderliche IT-Sicherheit zu gewährleisten, wenn diese nicht von Beginn an in der eingekauften Ubiquitous Computing-Technik eingebaut ist.[309] Eine vergleichbare Entwicklung zu einer mit einem Wissensdefizit behafteten verantwortlichen Stelle lässt sich auch im Bereich der neuen Computernutzer beobachten, die ein Gerät heute zu fast für jedermann erschwinglichen Preisen erwerben und innerhalb weniger Minuten an das Internet anschließen können. In der Regel verfügen solche Anwender aber nur über einen geringen Informationsstand zum Selbstschutz ihrer eigenen Daten sowie ihres Gerätes unter den Bedingungen einer offenen Netzumgebung. Ohne eine entsprechende Vorinstallation der notwendigen Tools und einer datenschutzfreundlichen Konfiguration der Voreinstellungen sind solche Anlagenbetreiber auch heute schon kaum in der Lage, ihren Verpflichtungen zur Gewährleistung einer angemessenen IT-Sicherheit nachzukommen.

Es bedarf mit anderen Worten proaktiver Maßnahmen, die eine Schadensentwicklung von Beginn durch standardisierte Lösungen unterbinden. Dies ist insbesondere auch deswegen erforderlich, weil die Verletzung von Sorgfaltspflichten oder das Fehlen von Sicherheitsmaßnahmen als Negativbeispiel öffentlich werden kann[310] und damit das Vertrauen in den konkreten Betreiber in Zweifel ziehen, aber auch die Akzeptanz von Ubiquitous Computing-Systemen generell vermindern kann.

Die IT-Sicherheit in Ubiquitous Computing-Anwendungen dient der Risiko- und damit Kostenminimierung von Ausfall- und Akzeptanzschäden. Bislang ist zweifelhaft, ob überhaupt technische Konzepte vorliegen, um hinreichende IT-Sicherheit in multilateralen Beziehungsgeflechten gewährleisten zu können, wie sie Ubiquitous Computing-Systeme insbesondere im Convenience-Beispiel darstellen. Ungeachtet dessen würde die Implementierung der er-

[308] Ansprüche auf Löschung oder Schadensersatz nach § 823 BGB bzw. § 1004 BGB.

[309] Zur Forderung eines verstärkten Datenschutzes durch Technik siehe Rossnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, S. 184.

[310] Wie unlängst der Diebstahl von mehreren hunderttausend Datensätzen von Kreditkartendaten in den USA, vgl. http://www.heise.de/newsticker/meldung/58733 (19.04.2005).

forderlichen IT-Sicherheit die Kosten der Anwendungen erhöhen. Bei der Einführung solcher Systeme ohne hinreichende Sicherheit läge jedoch ein Verstoß gegen Datenschutzrecht vor, der eine Risikoerhöhung auf Betreiberseite und damit einen beschränkenden Bestimmungsfaktor für Ubiquitous Computing darstellt.

3.4.3.2 Arbeitswelt

Von Anwendungen des Ubiquitous Computing verspricht sich insbesondere die Industrie relevante Einspar- und Rationalisierungseffekte, weil sie eine automatisierte Erkennung der Produkte und ihre Steuerung ermöglichen. Die automatisierte Erkennung und Zuordnungsmöglichkeit von Einzelprodukten ermöglicht es häufig auch, einzelne Arbeitnehmer für Teilschritte im Herstellungs- und Auslieferungsvorgang als verantwortlich zu identifizieren. Diese Zuordnungsmöglichkeit erlaubt Rückschlüsse auf die Arbeitsleistung dieser Arbeitnehmer. Jedoch unterliegt die Kontrolle der Arbeitsleistung von Arbeitnehmern arbeitsrechtlichen Vorschriften und ist insbesondere mitbestimmungspflichtig.

3.4.3.2.1 Rechtsrahmen

Das Arbeitsrecht umfasst die Summe der Rechtsregeln, die sich mit der in abhängiger Tätigkeit geleisteten Arbeit beschäftigen. Dabei geht es um die Regelung des Verhältnisses des Arbeitnehmers zum Arbeitgeber (Arbeitsvertrag, Individualarbeitsrecht) ebenso wie um das Verhältnis von Gruppen und Vertretern von Arbeitnehmern (z.B. Betriebsrat, Gewerkschaften, Tarifvertragsparteien) und Arbeitgebern (z.B. Arbeitgeberverbände) untereinander und zum Staat (kollektives Arbeitsrecht).[311] Drei große Bereiche bestimmen den Rechtsrahmen in der Arbeitswelt: Das Arbeitsrecht als Schutzrecht des Arbeitnehmers, das Tarifvertragswesen sowie das Betriebs- und Unternehmensverfassungsrecht.

Das Arbeitsrecht berührt eine Reihe von Vorgaben des Grundgesetzes (GG), so u.a. Art. 3 (Gleichberechtigung von Mann und Frau), Art. 5 (Meinungsäußerungsfreiheit), Art. 9 Abs. 2 (Koalitionsfreiheit), Art. 11 (Freizügigkeit) und Art. 12 Abs. 1 bis 3 (Freie Ausbildungs- und Berufswahl, Verbot von Zwangsarbeit). Auf einfachgesetzlicher Ebene ist es überwiegend als Bundesrecht ausgestaltet, auch wenn generell eine konkurrierende Gesetzgebung des Bundes und der Länder in diesem Bereich besteht (Art. 74 Nr. 12 GG). Darüber hinaus kommt autonomen, von den Organen des Arbeitslebens geschaffenen Rechtsnormen (wie u.a. Tarifverträgen, Betriebsvereinbarungen, Unfallverhütungsvorschriften) eine entscheidende Bedeutung zu. Auf europäischer Ebene sind einige der Grundfreiheiten und weitere Teile des Primärrechts auf arbeitsrechtliche Regelungsgegenstände gerichtet. Ferner gibt es eine große Zahl sekundärrechtlicher Regelungen.[312]

Der Einsatz von Systemen des Ubiquitous Computing berührt insbesondere die Frage der Überwachung von Arbeitnehmern durch die Nutzung von Datenbeständen, die durch Ubiquitous Computing-Systeme generiert werden. Die Frage der Arbeitnehmerkontrolle ist einer-

[311] Schaub, Arbeitsrechtshandbuch, § 2 Rn. 1.

[312] vgl. Schaub, Arbeitsrechtshandbuch, Rn. 93ff.

seits eine Frage des Arbeitnehmerdatenschutzes und damit bei den bereits erläuterten datenschutzrechtlichen Regelungen angesiedelt. Andererseits liegt der Schwerpunkt im Betriebsverfassungsrecht. Der § 87 Abs. 1 S. 6 Betriebsverfassungsgesetz (BetrVG) unterwirft die Einführung jeglicher technischer Maßnahmen, die „zur Arbeitnehmerkontrolle *bestimmt*" sind, dem Mitbestimmungsrecht des Betriebsrats. Die allgemein anerkannte Auslegung des Wortlauts dieser Norm geht aber noch weiter, indem alle Maßnahmen, die zur Kontrolle *geeignet* sind, mitbestimmungspflichtig sind.[313] Das bedeutet, dass Ubiquitous Computing-Systeme, soweit sie Datenbestände über Arbeitnehmer sammeln, die zur Arbeitskontrolle herangezogen werden können, nur mit Zustimmung des Betriebsrats oder nach Durchlauf eines Schlichtungsverfahrens eingeführt werden dürfen. Ein weiteres wichtiges Element des Arbeitsrechts ist die Betriebsvereinbarung. In Betriebsvereinbarungen können u.a. Maßnahmen der Arbeitnehmerkontrolle aber auch die Beschränkung (Durchsetzung einer strengen Zweckbindung) von grundsätzlich dazu geeigneten Systemen einvernehmlich zwischen dem Arbeitgeber und Arbeitnehmervertretern getroffen werden. Die Regelung der Zweckbestimmung von Ubiquitous Computing-Systemen und deren Datenbeständen in entsprechenden Betriebsvereinbarungen ist daher in jedem Fall geboten.[314]

3.4.3.2.2 Überwachung

Die oben beschriebenen Beispiele aus der Produktion und der Logistikkette zeigen, dass die Identifikationswirkung von Ubiquitous Computing und das Wissen um die interne Organisation von Produktion und Logistik eine umfassende Überwachung und Auswertung von Personen am Arbeitsplatz ermöglichen. Dies gilt zumindest dann, soweit das Verhalten der Arbeitnehmer sensorisch erfasst werden kann. Die Einführung derartiger Maßnahmen bietet die Möglichkeit der Leistungs- und Verhaltenskontrolle auf technischem Wege und ist daher mitbestimmungspflichtig gem. § 87 Abs. 1 Nr. 6 BetrVG.

Arbeitnehmervertreter verfügen damit über ein wirksames Mittel, um eine Anwendung von Ubiquitous Computing zur Leistungs- und Verhaltenskontrolle im Unternehmen zu unterbinden. Wenn Ubiquitous Computing-Systeme prinzipsbedingt nicht so gestaltet werden können, dass keine Datenbestände anfallen, die die Arbeitnehmerüberwachung ermöglichen, kann dies ihre Einführung im Unternehmen zeitlich hemmen oder sogar ganz verhindern. Insofern kann das Arbeitsrecht als beschränkender Faktor für diese Gruppe von Ubiquitous Computing-Systemen wirken.

3.4.3.3 Verbraucherschutz

Anwendungen des Ubiquitous Computing sollen den Abschluss und die Durchführung von Kaufverträgen über Waren oder Dienstleistungen vereinfachen und für den Anbieter kostengünstiger gestalten. Dabei beeinflussen sie den Auswahl-, Entscheidungs-, Zahlungs- und Auslieferungsvorgang als Einzelbestandteile des Kaufs. Das Verbraucherschutzrecht geht

[313] Gola / Wronka, Handbuch zum Arbeitnehmerdatenschutz, S. 424ff.

[314] vgl. auch Däubler, Computersysteme im Handel – rechliche Rahmenbedingungen für den Betriebsrat, S. 33 (36).

von dem Leitbild des „mündigen Verbrauchers“ aus[315], das einen fairen Leistungsaustausch beider Seiten durch Herstellung oder Erhalt eines Verhandlungsgleichgewichts anstrebt. Dementsprechend können verbraucherschützende Regelungen die Anwendungen im Ubiquitous Computing beeinflussen, wenn diese einseitige Vorteile für den Anbieter herstellen.

3.4.3.3.1 Rechtsrahmen

Das Verbraucherschutzrecht verfolgt verschiedene Zielrichtungen. Dazu gehört einerseits, den Kunden vor gesundheitlichen Schäden durch den Konsum von Waren und Dienstleistungen zu bewahren (Produktsicherheit), eine Irreführung des Verbrauchers zu vermeiden und Marktransparenz herbeizuführen. Andererseits soll auch die Schädigung oder Ausbeutung von Kunden verhindert werden, um Notlagen von Verbrauchern und damit eine sozialpolitische Schieflage zu verhindern.[316] Zur Erhaltung des Verhandlungsgleichgewichts zwischen Kunden und Anbietern enthält das Verbraucherrecht daher Anforderungen an die Transparenz gegenüber dem Verbraucher sowie Verbote, ihn zu übervorteilen, die Einfluss auf den Einsatz von Ubiquitous Computing im Konsumumfeld nehmen können.

Verbraucherrechtliche Vorgaben finden sich einerseits in Recht der Allgemeinen Geschäftsbedingungen, die mittlerweile in den §§ 312 ff. BGB in das Bürgerliche Gesetzbuch integriert sind. Regelungen des Anfechtungsrechts und der Nichtigkeit des allgemeinen Teils des BGB gehören ebenso dazu wie das Recht der Leistungsstörungen und die Sachmängelhaftung. Weitere Bereiche sind das Wettbewerbsrecht und die Produkthaftung. Auch für den Konsum von Dienstleistungen (was im Hinblick auf die Bereitstellung von Ubiquitous Computing-Anwendungen im Wege des Application Service Providing relevant werden könnte), im Miet-, Verbraucherkredit-, Versicherungs-, Reisevertragsrecht finden sich verbraucherschützende Vorschriften.[317] Das Lebensmittel- und Arzneimittelrecht können ebenso verbraucherschützende Wirkungen entfalten. Diese Aufzählung macht deutlich, dass das Verbraucherrecht eine Querschnittsmaterie durch große Teile der Rechtsordnung darstellt und damit an vielfältigen Punkten regelnd auf den Einsatz von Ubiquitous Computing-Anwendungen einwirken kann. Viele der genannten Bereiche sind durch europarechtliche Regelungen vorgegeben, die für den europäischen Binnenmarkt einheitliche Anforderungen des Verbraucherschutzes formulieren. Beispiele sind die AGB-Richtlinie 93/13/EG, die Fernabsatzrichtlinie 97/07/EG, die E-Commerce-Richtlinie 2000/31/EG.[318]

3.4.3.3.2 Informationsvorsprung des Anbieters

Ubiquitous Computing-Systeme wie im Shopbeispiel ermöglichen eine präzise automatisierte Auswertung des Kundeninteresses, wie dies heute allenfalls anhand von Clickstream-Daten im E-Commerce-Shop möglich ist.

---

[315] Borchert, Verbraucherschutzrecht, S. 1.

[316] Borchert, Verbraucherschutzrecht, S. 1.

[317] Vgl. im Einzelnen Borchert, Verbraucherschutzrecht, §§ 1 –14.

[318] Zu den europarechtlich motivierten Vorgaben des Ubiquitous Computing: SWAMI: Scenario Analysis and Legal Framework – First Results, S. 27f.

Darauf aufbauend lassen sich kontextbasierte auf den Verbraucher zugeschnittene Angebote unterbreiten. Eine solche Zielgenauigkeit ist unter Kostengesichtspunkten und im Hinblick auf die Schonung von Umweltressourcen zwar sinnvoll, sie nimmt dem Verbraucher aber den Blick auf das Gesamtangebot und lenkt seine Entscheidung nach den Wünschen des Anbieters. Das Leitbild des mündigen Verbrauchers, der auf Basis umfassender Information und der Analyse eigener Bedürfnisse die Kaufentscheidung trifft, ist damit aber schwer in Einklang zu bringen. Insofern verschiebt sich das Gleichgewicht zwischen den Anbietern und Verbrauchern zu Gunsten des Anbieters.

Das Verbraucherrecht arbeitet ebenso wie das Datenschutzrecht solchen Verschiebungen entgegen, um einen Leistungsaustausch zu fairen Konditionen zu ermöglichen. Ansatzpunkte bietet hier insbesondere das Wettbewerbsrecht.[319] Diese Entwicklung wird sich limitierend auf den Einsatz von solchen Ubiquitous Computing-Systemen auswirken, die zu einer Informations- oder Angebotsbeschränkung des Kunden auf der Basis der Auswertung seines Kundenverhaltens führen.

Darüber hinaus bestehen weitere verbraucherrechtliche Pflichten der Kundeninformation insbesondere im Fernabsatz- und E-Commerce-Bereich. Das Beispiel der einkaufenden Haushaltsgeräte zeigt, dass solche Verträge eine besondere Rolle im Kontext von Ubiquitous Computing spielen können. Die Erfüllung der Informationspflichten ist daher auch in diesen Kontexten umzusetzen, allerdings werden die Anbieter ihnen – vergleichbar mit dem elektronischen Vertragsschluss – kaum für jeden einzelnen Kaufakt, sondern allenfalls über Rahmenverträge nachkommen können.[320]

3.4.3.3.3 Nutzung von Verbrauchsprofilen

Kundendaten sind bereits heute ein marktfähiges und wertvolles Gut, soweit sie eine zielgerichtete und damit effektivere Kundenansprache ermöglichen.

Die Erstellung von Verbraucherprofilen in genaueren Kategorien und auf einer umfangreicheren Datenbasis in automatisierter Form ergibt sich bei vielen Ubiquitous Computing-Systemen prinzip- oder gestaltungsbedingt. Damit steigt der Wert solcher Profile weiter bei gleichzeitigem Sinken der Kosten der Erhebung. Dies könnte zu Verlockungen für die Provider von Ubiquitous Computing-Systemen führen, solche Profile als Mittel zur Gewinnmaximierung zu verwenden. Dabei ist zu berücksichtigen, dass die Bildung und die Auswertung solcher Profile an die Schranken des Verbraucherdatenschutzrechtes stößt.[321] Entsprechendes gilt für die Vermarktung von Informationen über das Verhalten einzelner Verbraucher. Diese Grenzen wirken sich auf die Verwendung und Weiterveräußerung personenbezogener Kundenprofile, die aus Ubiquitous Computing-Anwendungen stammen, als einem eigenen

[319] Wie schon § 7 UWG „Unzumutbare Belästigungen“, der die europäischen Vorgaben gegen SPAM aus der Richtlinie 2002/58/EG umsetzt und gleichzeitig datenschützenden Charakter hat.

[320] Praktisch ergeben sich hier ähnliche Probleme wie bei der datenschutzrechtlichen Transparenz, s.o. Kap. 3.4.3.1.4.

[321] Zur Bedeutung datensparsamer Technikgestaltung siehe Roßnagel, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR, 2004, S. 625 (631).

Geschäftsfeld erheblich beschränkend aus. Lediglich die Verwendung von Daten ohne Personenbezug ist hiervon nicht betroffen.

3.4.3.4 Umweltschutz

Viele der oben beschriebenen Anwendungsbeispiele im Ubiquitous Computing setzen auf Datenübertragungen ohne Kabel. Dies gilt zumindest für den unmittelbaren Umgebungsbereich der Betroffenen. Derzeit entwickelt sich hauptsächlich die Funktechnik für Daten mit unterschiedlichen Reichweiten (WLAN, WMAX, UMTS etc.) weiter. Dies wird dazu führen, dass eine Vielzahl von Sendern im unmittelbaren Umfeld von Menschen platziert sein wird. Sender stellen elektromagnetische Strahlungsquellen dar. Durch die Miniaturisierung kann auch die Erkennbarkeit solcher elektromagnetischer Strahlungsquellen eingeschränkt sein oder sogar gänzlich verschwinden. Der Einsatz solcher Strahlungsquellen ist im Umweltrecht geregelt.

3.4.3.4.1 Rechtsrahmen

Das Umweltrecht umfasst eine ganze Reihe von einfachgesetzlichen Normen, von denen für die hier zu klärende Fragestellung das Bundesimmissionsschutzgesetz von besonderer Bedeutung ist. Zweck dieses Gesetzes ist es, Menschen, Tiere und Pflanzen, den Boden, das Wasser, die Atmosphäre sowie Kultur- und sonstige Sachgüter vor schädlichen Umwelteinwirkungen zu schützen und dem Entstehen schädlicher Umwelteinwirkungen vorzubeugen (§ 1 BImSchG). Zu dem BImSchG sind eine ganze Reihe von konkretisierenden Ausführungsverordnungen erlassen worden, darunter die 26. Verordnung zum Bundesimmissionsschutzgesetz (26. BImSchV), die so genannte Elektrosmog-Verordnung. Sie setzt Grenzwerte zum Schutz der Bevölkerung vor elektromagnetischen Feldern.

3.4.3.4.2 Elektrosmog

Die Elektrosmog-Verordnung folgt weitgehend den Empfehlungen der internationalen Strahlenschutzkommission für nichtionisierende Strahlung (International Commission on Non-Ionizing Radiation (ICNIRP)). Die ICNIRP orientiert ihre Grenzwertempfehlungen im hochfrequenten Bereich an den so genannten thermischen Effekten, das heißt der Erwärmung biologischer Gewebe.

Nach medizinischen Erkenntnissen über tolerierbare Erwärmung wird diejenige Wärmeleistung ermittelt, die vom Temperaturregelungs- und Wärmetransportsystem des Körpers schadlos abgeführt werden kann. Die Grenzwerte für die Leistungsflussdichte werden so festgelegt, dass die resultierende Erwärmung mit einem hinreichenden Sicherheitsabstand unter der medizinisch tolerierbaren Erwärmung bleibt.[322]

Der Grenzwert in Deutschland ist frequenzabhängig (z.B. für die UMTS-Frequenz (ca. 2000 MHz) 10 000 mW/m²). Die Grenzwerte wie auch die Ermittlungsmethoden für die Grenzwerte unterscheiden sich von Land zu Land signifikant. Daraus können sich Hemnisse für den

[322] Forum Elektrosmog, http://www.forum-elektrosmog.de/forumelektrosmog.php/aid/114/cat/33/ (31.03.2006).

grenzüberschreitenden Handel mit entsprechenden Ubiquitous Computing-Systemen ergeben.

Inwieweit Funkverbindungen im Rahmen des Ubiquitous Computing die festgelegten Grenzwerte übersteigen könnten, ist heute noch nicht umfassend erforscht.[323] Zwar existieren z.B. Angaben über die Strahlungsabgabe von Mobiltelefonen, doch diese sind nur partiell mit Funkverbindungen im Rahmen von Ubiquitous Computing-Anwendungen vergleichbar. Heranzuziehen dürfte der bei der deutschen Methode zur Grenzwertbildung wichtige Faktor der Körpernähe der Strahlungsquelle sein. Auch gibt es Anzeichen dafür, dass z.B. die Anwesenheit einer vermehrten Anzahl von Sendern in einem für die Strahlung umschlossenen Raum (z.B. PKW) zu einer schnelleren Grenzwerterreichung führt. Weiterhin dürfte auch die notwendige Senderstärke für die Diensteerbringung Einfluss auf die mögliche Überschreitung von Grenzwerten haben. Gesicherte Erkenntnisse in diesem Bereich, die valide Rückschlüsse für die Elektrosmog-Situation beim Ubiquitous Computing zulassen, sind daraus jedoch nicht abzuleiten. Es bleibt deshalb als Ergebnis festzuhalten, dass umweltrechtliche Vorgaben bei einer stark funkbasierten Weiterentwicklung des Ubiquitous Computing einen limitierenden Faktor für das Ubiquitous Computing darstellen können.

3.4.3.5 Informations- und Telekommunikationsrecht

Im Rahmen der beschriebenen Ubiquitous Computing-Anwendungen spielt die Anbindung mittels Telekommunikation als einigen Teilfunktionalitäten des Ubiquitous Computing zugrunde liegende Technik eine wichtige Rolle. Hier ist z.B. der häusliche Bereich zu nennen, dessen breitbandige Datenanbindung eine Grundvoraussetzung für viele Dienste darstellen wird. Aber auch die Verknüpfung lokal mittels Sensorik gesammelter Daten mit Hintergrundsystemen wird die Telekommunikation zu einem Grundbaustein des Ubiquitous Computing machen. Das Telekommunikationsrecht regelt sowohl die technische Umsetzung als auch viele Einzelheiten der Erbringung von Telekommunikationsdienstleistungen.

3.4.3.5.1 Rechtsrahmen

Telekommunikationsrechtliche Vorgaben enthält bereits das Grundgesetz, wobei nur Art. 10 GG mit dem Fernmeldegeheimnis materiellrechtlichen Charakter hat. Darüber hinaus werden in Art. 73 Nr. 7 GG, Art. 80 Abs. 2 GG, Art. 87 f GG und Art. 143 b GG Kompetenzen zur Gesetzgebung, dem Erlass von Rechtsordnungen und zur Verwaltung des Post- und Fernmeldewesens verteilt.

Auf einfachgesetzlicher Ebene ist insbesondere das 2004 novellierte Telekommunikationsgesetz (TKG) von zentraler Bedeutung. Die Regelungsbereiche sind dabei äußerst vielfältig und reichen von technischen Fragen der Ermöglichung von Telekommunikation und der Interoperabilität über Fragen des Wettbewerbs, des Kundenschutzes, des Datenschutzes und des Fernmeldegeheimnisses bis hin zur Rundfunkübertragung und der Organisation einer

[323] Rund 6 Prozent der Bevölkerung fühlen sich laut einer Umfrage im Auftrag des BfS durch Mobilfunkanlagen in ihrer Gesundheit beeinträchtigt. Weitere Forschungsvorhaben im Bereich des Elektrosmog sind daher aufgesetzt worden und in Planung, vgl. BT-Drs. 15/4604.

staatlichen Aufsichtsinstanz. Dem zu Grunde liegt eine Vielzahl europäischer Regelungen[324], die die Öffnung und Liberalisierung des ursprünglich staatlich monopolistisch geprägten europäischen Telekommunikationsmarktes zum Ziel haben. Für den Bereich des Ubiquitous Computing können vor allem zwei Bereiche von bestimmender Relevanz sein:

3.4.3.5.2 Frequenzordnung

Wie in Kap. 3.4.3.4 zum Umweltschutz bereits dargelegt, wird die Funktechnik eine entscheidende Rolle für die Funktionalität von Ubiquitous Computing-Systemen einnehmen. Dabei werden mit zunehmender Durchsetzung solcher Systeme immer mehr Frequenzen benötigt werden, um die störungsfreie parallele Funktion der Anwendungen sicherzustellen. Die Anzahl für bestimmte Reichweiten nutzbarer Frequenzen ist aus physikalischen Gründen begrenzt. Die Doppelnutzung einer Frequenz kann zu Störungen führen, so dass die Störungsfreiheit durch ein exklusives Nutzungsrecht bzw. die Ausschließung anderer Nutzer gesichert werden muss.[325] Zur Vermeidung von Verteilungskonflikten und zur Sicherstellung der Störungsfreiheit reguliert das Telekommunikationsrecht die Frequenzverwendung in den §§ 52-77 TKG, wobei insbesondere die §§ 52-60 und 63-65 TKG für die Funkfrequenzen Anwendung finden. Eine Vielzahl von Frequenzbereichen ist bereits durch den Frequenzbereichszuweisungsplan für bestimmte Anwendungsfelder vergeben, so dass derzeit vorwiegend nur kleine zulassungsfreie Frequenzbereiche für Ubiquitous Computing-Anwendungen zur Verfügung stehen.

Die Belegung genehmigungspflichtiger Frequenzen ist zwar ebenfalls denkbar. Sie würde aber die Kosten der Ubiquitous Computing-Anwendung erhöhen. Eine solche Nutzung ist vor allem für Anwendungen denkbar und auch geboten, die in kritischen Infrastrukturen eingesetzt werden, weil Störungsfreiheit und Verfügbarkeit in diesen Fällen eine sehr hohe Priorität haben.

Bei einem massenhaften Einsatz von Ubiquitous Computing-Systemen können sich aus der begrenzten legal verwendbaren Frequenzanzahl faktische Beschränkungen (quantitativ und regional) ergeben, die die Funktionalität und damit Verbreitung des Ubiquitous Computing einschränken.

3.4.3.5.3 Telekommunikationsdienste

Für Ubiquitous Computing-Systeme gilt, dass zwischen Transpondern und Sensoren bzw. Lesegeräten der Hintergrundsysteme Signale über Funkfrequenzen ausgesendet, übermittelt und empfangen werden. Um Telekommunikation im Sinne von § 3 Nr. 22 TKG handelt es sich jedoch erst dann, wenn diese technischen Vorgänge definitionsgemäß auch über eine Telekommunikationsanlage erfolgen. Dies sind nach § 3 Nr. 23 TKG technische Einrichtungen oder Systeme, die die Signale übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Diese Funktionalität wird in Ubiquitous Computing-Systemen im Regelfall von den über ein Hintergrundsystem verbundenen Sensoren bzw. Prozessoren erfüllt, die die

[324] Koenig / Loetz / Neumann, Telekommunikationsrecht, S. 49ff.

[325] Koenig / Loetz / Neumann, Telekommunikationsrecht, S. 176ff.

Transponder ansteuern, die Informationen auslesen oder im Fall aktiver Transponder auch übertragen.[326]

Die Anwendung vieler Regelungen des Telekommunikationsgesetzes basiert jedoch auf dem Vorliegen eines Telekommunikationsdienstes. So ist bspw. jeder „Dienstanbieter" nach § 88 Abs. 2 Satz 1 TKG zur Wahrung des Fernmeldegeheimnisses verpflichtet. Diesem ist es nach § 88 Abs. 3 Satz 1 untersagt, dass er sich oder anderen „über das für das geschäftsmäßige Erbringen der Telekommunikationsdienste, einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus, Kenntnis von Inhalt und näheren Umständen der Telekommunikation verschafft". Nach der gesetzlichen Definition in § 3 Nr. 24 TKG ist ein Telekommunikationsdienst ein in der Regel gegen Entgelt erbrachter Dienst, der ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht. Geschäftsmäßig wird dieser Telekommunikationsdienst erbracht, wenn er nachhaltig für Dritte mit oder ohne Gewinnerzielungsabsicht angeboten wird (§ 3 Nr. 10 TKG). Telekommunikationsnetze sind nach § 3 Nr. 27 TKG die „Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeeinrichtungen sowie anderweitiger Ressourcen, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen". Werden für die Kommunikation zwischen Lesegeräten bzw. Hintergrundsystemen und Transpondern lediglich freie Frequenzen genutzt, so fehlt es an einem Dienstanbieter, der eine „Transportdienstleistung" zwischen Absender und Empfänger erbringt.[327] Dies wäre erst dann der Fall, wenn der Informationsaustausch zwischen Lesegerät bzw. Hintergrundsystem und Transpondern über von einem Anbieter betriebenes Funknetz erfolgen würde. Dieser Anbieter wäre dann nach § 88 Abs. 2 TKG zur Wahrung des Fernmeldegeheimnisses verpflichtet. In diesem Fall wäre der Dienstanbieter aber auch verpflichtet, die Übermittlung auf der Funkstrecke, insbesondere das Fernmeldegeheimnis, durch „angemessene technische Vorkehrungen oder sonstige Maßnahmen" zu schützen (§ 109 Abs. 1 TKG).

Von Bedeutung kann jedoch in jedem Fall das Verbot nach § 89 Satz 1 TKG sein, über Funkanlagen vermittelte Nachrichten nicht unbefugt abzuhören. Eine Funkanlage ist eine Telekommunikationsanlage im Sinne des § 3 Nr. 23 TKG, die Nachrichten über Funkfrequenzen sendet, vermittelt und empfängt. Diese Voraussetzung erfüllen die Lesegeräte bzw. ihre Hintergrundsysteme. Nach der gesetzlichen Regelung in § 89 Satz 1 TKG dürfen nur die Nachrichten abgehört werden, die für den Betreiber der Funkanlage, Funkamateure, die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind. Diese Voraussetzung erfüllt die Funkkommunikation zwischen Lesegerät und Transponder regelmäßig nicht, sondern die Lesegeräte lesen und übermitteln Informationen aus bzw. an den Transponder, die sich im Sende- und Empfangskreis des Lesegerätes befinden.[328] Es handelt sich also regelmäßig um eine bidirektionale Kommunikation zwischen zwei Punkten, die aus diesem Grund

[326] Müller, Ist das Auslesen von RFID-Tags zulässig? DuD, 2004, 216.

[327] Ebenso Müller, Ist das Auslesen von RFID-Tags zulässig? DuD, 2004, 216.

[328] Ibid.

nicht abgehört werden darf. Soweit Lesegeräte „ungewollt“ Transponder erfassen, die sich in ihrem Empfangs- und Sendekreis befinden, ohne sie gezielt auszulesen und ihre Informationen zu speichern, gilt das Verbot der weiteren Verwendung dieser Informationen nach § 89 Satz 2 TKG.[329]

Die Anforderungen des Telekommunikationsrechts werden die Entwicklung von Ubiquitous Computing-Anwendungen nur insofern beschränken als Aufwendungen zum Schutz der Funkkommunikation zwischen Lesegerät und Transpondern erforderlich sein können. Dieser Aufwand wird maßgeblich von der Bedeutung (Personenbezug) und dem Wert der zwischen dem Lesegerät bzw. seinem Hintergrundsystem sowie den Transpondern ausgetauschten Informationen abhängen.

3.4.3.5.4 Zugangskontrolle

Anwendungen des Ubiquitous Computing werden in der Regel auf Grund eines Mehrwerts angeboten werden, da Anschaffung und Betrieb Kosten verursachen. Solche Mehrwerte sind beispielsweise Musik oder Bilder. Sie sollen in der Regel gezielt nur denen zukommen, die für ihre Inanspruchnahme auch bezahlt haben. Damit wird sich die Notwendigkeit ergeben, den Zugang zu einer solchen Medienanwendung zu kontrollieren, um einer wirtschaftlichen Entwertung des Angebotes vorzubeugen.[330] Der technische Mechanismus, mit dem die erlaubte Nutzung eines zugangskontrollierten Dienstes ermöglicht wird, wird auch als Zugangskontrolldienst bezeichnet (§ 2 Nr. 2 Zugangskontrolldiensteschutz-Gesetz – ZKDSG). Das auch als „lex premiere“ bekannte Gesetz sichert derartige technische Zugangskontrollsysteme, indem es die Umgehung solcher Systeme strafrechtlich sanktioniert (§ 4 i.V.m. § 3 ZKDSG).[331] Soweit über Ubiquitous Computing-Systeme Anwendungen angeboten und genutzt werden, die nach dem Willen des Anbieters nur für einen definierten Nutzerkreis zugänglich sein sollen und deshalb durch technische Verfahren den Zugang zu diesem Angebot kontrollieren, finden die strafrechtlichen Sanktionen für die Umgehung dieser Dienste Anwendung. Derartige Zugangskontrolldienste sind vor allem im Convenience-Bereich zu vermuten.

Zugangskontrollsysteme dienen der Einnahmesicherung aus Ubiquitous Computing-Anwendungen und können eine zusätzliche Schutzebene bilden zwischen dem Betreiber des Systems und seinem Nutzer. Vergleichbar der Entwicklung zum Schutz von Urheberrechten (siehe Kap. 3.4.3.8) können sie allerdings auch Anreize bilden, den jeweiligen Schutzmechanismus zu unterlaufen und auf diese Weise die Verbreitung von Medieninhalten über Ubiquitous Computing-Anwendungen zu bremsen.

---

[329] Ibid.

[330] SWAMI: Scenario Analysis and Legal Framework – First Results, S. 29f.

[331] Zur strafrechtlichen Dimension des Ubiquitären Computing siehe auch Eisenberg / Puschke / Singelnstein, Überwachung mittels RFID-Technologie, ZRP, 2005, S. 9-12.

3.4.3.6 Haftung

Da die Fehlerfreiheit von Technik nicht mit absoluter Sicherheit hergestellt werden kann, stellt sich die Frage, wer bei einem Versagen von Ubiquitous Computing-Systemen für möglicherweise auftretende Schäden haftet. Diese Frage stellt sich in besonderer Weise bei dem Einsatz von Ubiquitous Computing-Systemen in kritischen Infrastrukturen, da hier erhebliche Schäden auftreten können. Die Antwort auf derartige Fragen nach den Verantwortlichkeiten ergibt sich aus den Grundregeln des Haftungsrechts.

3.4.3.6.1 Rechtsrahmen

Die Anwendung von Haftungsnormen richtet sich nach ihrer Anwendung in konkreten Situationen und den Beteiligten. So haften Hersteller von Produkten nach dem Produkthaftungsgesetz (ProdhaftG) grundsätzlich für Personenschäden und eingeschränkt auch für Sachschäden, die ihre Produkte auslösen. Für den Hersteller bestehen jedoch Möglichkeiten zur Enthaftung, wenn er ein auf seiner Seite fehlendes Verschulden nachweisen kann. Diese Regelung könnte für die Hersteller nachhaltig von Bedeutung sein, soweit Ubiquitous Computing-Systeme als Produkte im Sinne von § 2 ProdhaftG anzusehen sind. Produkt im Sinne dieses Gesetzes ist jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet, sowie Elektrizität. Soweit also bewegliche körperliche Gegenstände (z.B. das Versagen von Sensoren) für einen Schaden verantwortlich sind, wird die Produkthaftung greifen. Etwas anderes dürfte gelten, wenn Schäden im Rahmen einer Dienstleistung beispielsweise bei der falschen Verknüpfung von Datenbeständen eintreten (z.B. Falschbeurteilung einer Situation durch das System auf Grund falscher Datenbestände). Hier wird auf allgemeine haftungsrechtliche Tatbestände wie z.B. § 823 Abs. 2 BGB zurückzugreifen sein, der eine verschuldensabhängige Haftung[332] je nach Schadenshöhe und Verursacher vorsieht.

Darüber hinaus ist an spezialgesetzliche Haftungsregelungen wie die datenschutzrechtliche Haftung nach § 7 BDSG zu denken.[333] In Ubiquitous Computing-Systemen in PKW-Anwendungen könnten auch die Regelungen zur Haftung bei Unfällen im Straßenverkehr gem. Straßenverkehrsgesetz bzw. der Straßenverkehrsordnung (StVG, StVO) in Betracht kommen. Diese sind als eine Gefährdungshaftung ausgelegt, wobei sich je nach Anwendung die Frage stellt, ob sie einen Bezug zum Straßenverkehr aufweist. Für Schäden an Ubiquitous Computing-Systemen dürfte, soweit es sich dabei um Produkte handelt, die allgemeine Gewährleistung über Sachmängel oder aber Garantieversprechen der Hersteller eingreifen.

Die Realisierbarkeit von Haftungsansprüchen ist insbesondere von der Beweislage abhängig. Die maßgebliche Ausgangsfrage ist danach erstens, wer muss welche Tatsache vor Gericht beweisen, und zweitens, ob eine Haftung des Schädigers sein Verschulden voraussetzt. Im Hinblick auf den Einsatz von Ubiquitous Computing-Systemen können dabei je nach Situation, Geschädigten und Schädigern unterschiedliche Haftungsnormen eine

[332] Thomas in Palandt, Bürgerliches Gesetzbuch, § 823 Rn. 54ff.

[333] Zur datenschutzrechtlichen Haftung vgl. auch Rossnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, 178ff., 184.

Rechtsfolge auslösen.

3.4.3.6.2 Risikomanagement

Fehlfunktionen in Ubiquitous Computing-Systemen (falsche Daten, keine Aktionen etc.) können zu materiellen und immateriellen Schäden am Produkt selbst oder zu Folgeschäden beim Geschädigten führen, die von den Verantwortlichen gegenüber den Geschädigten nach den Regelungen des Haftungsrechts auszugleichen sind.

Schadensfälle können außerdem zu einem Vertrauensverlust in die Leistungsfähigkeit der Ubiquitous Computing-Anwendung sowie ihres Anbieters führen. Derartige Imageschäden haben vor allem Bedeutung, wenn kritische Infrastrukturen von Schadensfällen betroffen sind. In diesen Fällen erhöhen sich zum einen die Schäden regelmäßig durch Folgeschäden, zum anderen gewinnt die Beeinträchtigung oder der Ausfall von kritischen Infrastrukturen regelmäßig eine höhere soziale und mediale Aufmerksamkeit in der Öffentlichkeit und kann als strukturelle Bedrohung wahrgenommen werden. Vorsorgliche Aufwendungen zur Risikominimierung werden zwar die Kosten der Anwendung erhöhen, sie stärken aber das Vertrauen und damit die Akzeptanz der Nutzer.

3.4.3.6.3 Verantwortlichkeit

Die haftungsrechtliche Verantwortung hängt von der Ausgestaltung des konkreten Ubiquitous Computing-Systems ab, welches für einen Schadensfall verantwortlich gemacht wird. Je höher die Komplexität des Systems, desto schwieriger die Beweisführung für den Geschädigten: Er muss den Verursacher benennen und eine Kausalität zwischen einem Fehler und dem Schaden beweisen. Der Verzicht auf die Regulierung von Schäden wird die Verantwortlichen vor Verlusten bewahren, aber umgekehrt stärken Situationen einer strukturellen Verantwortungslosigkeit nicht das Systemvertrauen, sondern beschränken die Entwicklung des Ubiquitous Computing.

Eine noch offene Frage ist die Verteilung der Verantwortlichkeit von unterschiedlichen Beteiligten an Ubiquitous Computing-Systemen (Benutzer, Provider, Importeur, Hersteller), wenn die Ursache für das Versagen nicht mehr mit Sicherheit zu ermitteln ist. Hier kann eine Gefährdungshaftung, wie sie beim Betrieb potentiell gefährlicher Maschinen (z.B. PKW) angenommen wird, Schäden der Betroffenen kompensieren, aber auch die Kosten für Ubiquitous Computing-Systeme erhöhen.

3.4.3.7 Internationalität

Die Sensoren der Ubiquitous Computing-Systeme sowie die Verknüpfung von Kontextinformationen sind nicht an nationale Grenzen und Rechtssysteme gebunden. Im normalen Einsatz wie auch im Schadensfall wirft der grenzüberschreitende Einsatz Fragen nach dem jeweils anwendbaren Recht auf. Dies gilt insbesondere, wenn Ubiquitous Computing-Anwendungen als Application Service Providing international erbracht werden.

Solche Fragen werden entweder durch internationale Mindeststandards oder aber durch das

so genannte Kollisionsrecht beantwortet, das über das anwendbare Recht entscheidet. Dies ist für den zivilrechtlichen Bereich umfänglich im Einführungsgesetz des BGB kodifiziert.[334] Die dortigen Regelungen kommen zu sehr differenzierten Antworten, die von dem betroffenen Rechtsgebiet und diversen weiteren Faktoren wie z.B. der Verbrauchereigenschaft des Betroffenen abhängen.

Unklarheiten werden hier zur Rechtsunsicherheit führen. Ohne eine strukturelle Klärung der Verantwortlichkeit in internationalen Anwendungsfeldern wird der Einsatz von Ubiquitous Computing auf Akzeptanzhindernisse stoßen.[335]

3.4.3.8 Verwertungsrecht

Wie die dargestellten Ubiquitous Computing-Anwendungen aufzeigen, können im Rahmen von Ubiquitous Computing-Diensten auch mit Rechten behaftete Objekte (Bilder, Filme, Musik, Klingeltöne etc.) genutzt, konsumiert und ausgetauscht werden. Gegenstände die mit geistigen Eigentumsrechten behaftet sind, können nur auf vertraglicher oder gesetzlicher Grundlage genutzt oder weitergegeben werden. Rechtliche Regelungen für diese Fälle enthält beispielsweise das Urhebergesetz oder das Patentgesetz.

3.4.3.8.1 Rechtsrahmen

Rechte an geistigem Eigentum existieren einerseits in Form von Urheberpersönlichkeitsrechten, die dem Urheber direkt zustehen, andererseits auch durch Übertragung von Rechten im Wege des Urhebervertragsrechts.[336] In diesem Zusammenhang versuchen Erwerber von Rechten (z.B. die Musik- oder Filmindustrie) diese möglichst gewinnbringend weiterzuveräußern. Die kommerzielle Verwertung digitaler Inhalte, die im Rahmen von Ubiquitous Computing-Systemen übertragen werden können, ist mit dem besonderen Problem der verlustfreien Kopierbarkeit elektronischer Inhalte behaftet. Diesem versuchen Rechteverwerter und Urheber mit technischen Maßnahmen, dem so genannten Digital Rights Management, zu begegnen.[337] Die bisherigen Umsetzungen solcher Systeme werfen eine Vielzahl insbesondere datenschutzrechtlicher Fragestellungen auf.[338] Ihre technische Wirksamkeit und ihre Funktionsfähigkeit im Markt sind bisher nicht erwiesen, weshalb auch für den Bereich des Ubiquitous Computing die Vergütungsproblematik für Inhalte als nicht gelöst angesehen werden muss.

---

[334] Heldrich in Palandt, Bürgerliches Gesetzbuch, Einl v EGBGB, Rn. 1ff., 5.

[335] Die Fragen der Verantwortlichkeit werden in Arbeitspaket 5 unter dem Gesichtspunkt rechtlicher Lösungen näher untersucht werden.

[336] Zum Urheberrecht: Hoeren, Skript zum Informationsrecht, S. 52ff.

[337] Grimm / Puchta, Datenspuren bei der Nutzung von DRM, DuD, 2006, S. 74ff. IDMT/ULD/TU Ilmenau, Privacy4DRM, Studie im Auftrag des BMBF, 2005; Hansen, Markus, DRM Desaster: Das Sony BMG-Rootkit, DuD 2006, S. 95ff.; Spielkamp, Was kaufe ich im Online-Musikgeschäft?, DuD 2006, S. 90ff.

[338] Vgl. Bizer / Grimm / Will, Nutzer- und Datenschutzfreundliches DRM, DuD 2006, S. 69ff.; Möller / Bizer, Datenschutzrechtliche Anforderungen an DRM, DuD 2006, S. 80ff.; IDMT/ULD/TU Ilmenau, Privacy4DRM, Studie im Auftrag des BMBF, 2005.

3.4.3.8.2 Nachvollziehbarkeit

Die Rechteinhaber werden einer Verwertung ihrer Inhalte in digitaler Form im Rahmen von Ubiquitous Computing-Systemen nur dann zustimmen, wenn die Nutzung ihrer Rechte nachvollziehbar ist und damit Entgelte liquidiert werden können. Ohne attraktive Inhalte wird die Entwicklung entsprechender Ubiquitous Computing-Systeme begrenzt sein, so dass eine Nachvollziehbarkeit der Nutzung digitaler Inhalte innerhalb von Ubiquitous Computing-Systemen für eine ungehinderte Entwicklung notwendig ist.[339] Die gleichzeitige Wahrung der Datenschutzrechte der Nutzer stellt dabei eine besondere Hersausforderung dar.[340]

[339] IDMT/ULD/TU Ilmenau: Privacy4DRM, Studie im Auftrag des BMBF, 2005; Will / Jazdzejewski / Weber: Kundenfreundlichkeit von Musik Downloadplattformen, DuD, 2006, S. 85ff.

[340] Näher Bizer / Grimm / Will, DuD, 2006, S. 69ff.; Möller / Bizer, DuD, 2006, S. 80ff. IDMT/ULD/TU Ilmenau, Privacy4DRM, Studie im Auftrag des BMBF, 2005.

3.4.4 Literatur

Bizer, Johann / Grimm, Rüdiger / Will, Andreas: Nutzer- und Datenschutzfreundliches Digital Rights Management, Datenschutz und Datensicherheit (DuD), 2006, 69-73.

Barthel, Thomas: RFID-Anwendungen im Betrieb und bei Arbeitnehmerdaten, Datenschutznachrichten (DANA), 03/2004, S. 5-9.

Borchert, Günter: Verbraucherschutzrecht, München 1994.

Bundesverfassungsgericht (BVerfG): „Lauschangriff“, 1 BvR 2378/98 vom 03.03.2004.

Bundesverfassungsgericht (BVerfG): „Volkszählung“, BVerfGE 65, S. 1.

Däubler, Wolfgang: Computersysteme im Handel – rechtliche Rahmenbedingungen für den Betriebsrat, in: Die Zukunft im Handel hat begonnen! RFID, PEP, Loss Prevention & Co, Dokumentation zur Fachtagung der BTQ Kassel und ver.di Fachbereich Handel, 15.-17. November 2004, S. 33-38.

Deutsch, Erwin: Die neuere Entwicklung der Rechtsprechung zum Haftungsrecht, Juristenzeitung (JZ) 2005, S. 987-994.

Deutscher Bundestag: Bericht der Bundesregierung über die Forschungsergebnisse in Bezug auf Emissionsminderungsmöglichkeiten der gesamten Mobilfunktechnologie und in Bezug auf gesundheitliche Auswirkungen, Bundestagsdrucksache 15/4604 vom 27.12.2004.

Deutscher Bundestag: Eintrittskarten zur Fußball-Weltmeisterschaft 2006 und Datenschutz (Kleine Anfrage), Bundestagsdrucksache 15/4896 vom 16.02.2005.

Deutscher Bundestag: Eintrittskarten zur Fußball-Weltmeisterschaft 2006 und Datenschutz (Antwort der Bundesregierung), Bundestagsdrucksache 15/5011 vom 07.03.2005.

Conrad, Isabell: RFID-Ticketing aus datenschutzrechtlicher Sicht, Computer und Recht (CR) 2005, S. 537ff.

Eisenberg, Ulrich / Puschke, Jens / Singelnstein, Tobias: Überwachung mittels RFID-Technologie, ZRP, 01/2005, S. 9-12.

Forum Elektrosmog: Grenzwerte im internationalen Vergleich, http://www.forum-elektrosmog.de/forumelektrosmog.php/aid/114/cat/33/ vom 14.05.2005.

Fraunhofer-Institut für Digitale Medientechnologie (IDMT) / Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) / Institut für Medien- und Kommunikationswissenschaft der TU Ilmenau: Privacy4DRM, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, Mai 2005, http://www.datenschutzzentrum.de/drm/privacy4drm.pdf (29.03.2006).

Gola, Peter / Wronka, Georg: Handbuch zum Arbeitnehmerdatenschutz, 3. Aufl., Frechen 2004.

Gola, Peter / Schomerus, Rudolf: BDSG, Bundesdatenschutzgesetz, Kommentar, 8. Aufl., München 2004.

Grimm Rüdiger / Puchta, Stefan: Datenspuren bei der Nutzung von Digital Rights Management Systemen (DRM), Datenschutz und Datensicherheit (DuD) 2006, 74-79.

Hansen, Markus: DRM-Desaster: Das Sony BMG-Rootkit, Datenschutz und Datensicherheit (DuD), 2006, 95-97, http://www.datenschutzzentrum.de/drm/DuD(2)2006-Hansen.pdf (29.03.2006).

Heise Newsticker: Bundesregierung: RFID-Chips für Masseneinsatz geeignet, http://www.heise.de/newsticker/meldung/75963 (19.07.2006).

Heise Newsticker: Fußball-WM: Lückenlose Kontrolle gescheitert, http://www.heise.de/newsticker/meldung/74140 (12.06.2006).

Heise Newsticker: Fußball-WM: OK hält personalisiertes Ticketing für sinnvoll, http://www.heise.de/newsticker/meldung/74917 (30.06.2006).

Heise Newsticker: Fußball-WM: Zur EM wird alles anders,

http://www.heise.de/newsticker/meldung/74448 (20.06.2006).

Heise Newsticker: Pervasive 2005: Realitätsabgleich, http://www.heise.de/newsticker/meldung/59440 (10.05.2005).

Heise Newsticker: Bundesdatenschützer will keine gläsernen Autofahrer, http://www.heise.de/newsticker/meldung/71439 (29.03.2006).

Hilty, Lorenz: Beitrag zum 1. TAUCIS Projektworkshop

Hoeren, Thomas: Skript zum Informationsrecht, Stand März 2005, http://www.uni-muenster.de/Jura.itm

Holznagel, Bernd / Bonnekoh, Mareike: Radio Frequency Identification – Innovation vs. Datenschutz? MultiMedia und Recht (MMR), 2006, S. 17-23.

Hülsmann, Werner: RFIDs – Bleibt der Datenschutz auf der Strecke? Datenschutznachrichten (DANA), 04/2004, S. 11-15.

Internationale Konferenz der Datenschutzbeauftragten: Entschließung zu Radio-Frequency Identification vom 20.11.2003, http://www.privacyconference2003.org/resolutions/RFIDResolutionGE.doc

ISTAG (Ducatel, K. / Bogdanowicz, M. / Scapolo, F. / Leijten, J. / Burgelman, J-C.): Scenarios for Ambient Intelligence in 2010 – Final Report, February 2001, http://www.cordis.lu/ist/istag.htm (25.10.2005).

Kelter, Harald / Widmann, Stefan: Radio Frequency Identification – RFID , Datenschutz und Datensicherheit (DuD), 2004, S. 331-334.

Koenig, Christian / Loetz, Sascha / Neumann, Andreas: Telekommunikationsrecht, Heidelberg 2004.

Lahner, Claus Mauricio: Anwendung des § 6 c BDSG auf RFID, Datenschutz und Datensicherheit (DuD) 2004, S. 723-726.

Landesarbeitskreis Demokratie & Recht von Bündnis90 / Die Grünen Bayern: Gebrauch von RFID-Chips reglementieren, Resolution vom 23.03.2005, http://www.bayern.gruene-partei.de/cms/themen/dokbin/67/67416.rfid_chips_reglementieren_maerz_2005.pdf (29.03.2006).

Langheinrich, Marc: Die Privatspäre im Ubiquitous Computing, http://www.vs.inf.eth.ch/publ/papers/langhein2004rfid.pdf (29.03.2006).

Meyer, Jan-Bernd: Wie RFID funktioniert – und wie nicht, Computerwoche (CW), 25/2005, S. 22-23.

Möller, Jan / Florax, Björn-Christoph: Datenschutzrechtliche Unbedenklichkeit des Scoring von Kreditrisiken? Neue Juristische Wochenschrift (NJW), 2003, S. 2724-2726.

Möller, Jan / Florax, Björn-Christoph: Kreditwirtschaftliche Scoring-Verfahren, MultiMedia und Recht (MMR), 2002, S. 806-810.

Möller, Jan / Bizer, Johann: Datenschutzanforderungen an Digital Rights Management, Datenschutz und Datensicherheit (DuD), 2006, 80-84.

Müller, Jürgen: Ist das Auslesen von RFID-Tags zulässig? – Schutz von RFID-Transponderinformationen durch § 86 TKG, Datenschutz und Datensicherheit (DuD), 2004, S. 215-217.

Müller, Jürgen / Handy Matthias: RFID und Datenschutzrecht, Risiken, Schutzbedarf und Gestaltungsideen, Datenschutz und Datensicherheit (DuD), 2004, S. 655-659.

Ohlenburg, Anna: Der neue Telekommunikationsdatenschutz, MultiMedia und Recht (MMR), 2004 S. 431ff.

Palandt, Bürgerliches Gesetzbuch, 61. Aufl. München 2002.

Protokoll zum 1. TAUCIS Workshop.

Roßnagel, Alexander, Pfitzmann, Andreas, Garstka, Hansjürgen: Modernisierung des Datemschutzrechts, Gutachten im Auftrag des Bundesministerium des Innern, Berlin 2001.

Roßnagel, Alexander, Müller, Jürgen: Ubiquitous Computing – neue Herausforderungen für den Da-

tenschutz, Computer und Recht (CR), 08/2004, S. 625-632.

Roßnagel, Alexander: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MultiMedia und Recht (MMR), 02/2005, S. 71-75.

Saeltzer, Gerhard: Sind diese Daten personenbezogen oder nicht? Datenschutz und Datensicherheit (DuD), 2004, S. 218-227.

Schaar, Peter: Datenschutzbeauftragter Peter Schaar warnt vor blauäugiger RFID-Nutzung, Interview in Computerwoche (CW), 25/2005, S. 25.

Schaub, Günter: Arbeitsrechtshandbuch, 9. Aufl., München 2000.

Schoen, Thomas: Rechtliche Rahmenbedingungen zur Analyse von Log-Files, Datenschutz und Datensicherheit (DuD), 2005, S. 84-88.

Safeguards in a World of Ambient Intelligence (SWAMI), (Friedewald, Michael, Wright, David (Hrsg.)): Scenario Analysis and Legal Framework – First Results, Vers. 1.0 vom 24.05.2005.

Senate Bill of the State of California: No. 1834 of February 20, 2004.

Simitis, Spiros, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., München 2003.

Spielkamp, Matthias, Was kaufe ich im Online-Musikgeschäft, Datenschutz und Datensicherheit (DuD), 2006, 90-94, http://www.datenschutzzentrum.de/drm/DuD(2)2006-Spielkamp.pdf (29.03.2006).

Tangens, Rena / Rosengart, Frank: BigBrotherAward 2003 – Verbraucherschutz, Datenschutznachrichten (DANA) 04/2003, S. 8-10.

Gräfin von Westerholt, Margot / Döring, Wolfgang: Datenschutzrechtliche Aspekte der Radio Frequency Identification, Computer und Recht (CR), 2004, S. 710ff.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, Gutachten, Kiel 2005, http://www.bmelv.de/cln_045/nn_752314/SharedDocs/downloads/02-Verbraucherschutz/Finanzdienstleistungen/scoring,templateId=raw,property=publicationFile.pdf/scoring.pdf (29.03.2006).

Weichert, Thilo: Identitätskarten – sind Sicherheit und Datenschutz möglich? http://www.datenschutzzentrum.de/vortraege/050428_weichert_alcatel.htm (29.04.2005).

Weichert, Thilo: Die Fußball-WM als Überwachungs-Großprojekt, Datenschutznachrichten (DANA), 01/2005, S. 7-11.

Weiser, Mark: The Computer for the 21st Century, http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html (11.05.2005).

Will, Andreas / Jazdzejewski, Stefan / Weber, Anja, Kundenfreundlichkeit von Musik-Downloadplattformen, Datenschutz und Datensicherheit (DuD), 2006, 85-89.

4 Szenarien

Markus Hansen, Benjamin Fabian, Jan Möller, Sarah Spiekermann

4.1 Einleitung

Viele Faktoren beeinflussen die weitere Entwicklung des Ubiquitous Computing. Es ist daher problematisch, genaue Vorhersagen für den zeitlichen Verlauf und die Ausgestaltung einzelner Anwendungen zu prognostizieren. Die folgenden Szenarien sollen daher exemplarische Einblicke in das Leben in verschiedenen Welten des Ubiquitous Computing geben, wobei die im vorherigen Kapitel dargestellten Bestimmungsfaktoren implizit in die Darstellung einfließen. Am rechten Rand finden sich jeweils Hinweise, welche Aspekte des UC ins jeweilige Szenario gerade einfließen.

4.2 Szenario 1: Alltag

Piep, Piep, Pieeeeeeeep. „Guten Morgen! Zeit zum Aufstehen!“ Eine freundliche weibliche Stimme erfüllte den langsam heller werdenden Raum.

Flexible Konfigurierbarkeit

„Zum Unterbrechen der Weckfunktion für zehn Minuten klatschen Sie bitte dreimal in die Hände.“ Björn blinzelte. Nachdem er zum dritten Mal einen Termin verpasst hatte, weil er seinen Wecker im Schlaf abschalten konnte, hatte er sich von einem Bekannten diese neue interaktive Weckfunktion im Haus-System installieren lassen. Jeden Morgen wurde ihm nun eine neue Aufgabe zugewiesen und auch heute wurde er dadurch rechtzeitig wach.

Kontextadaptivität

Während er aufstand, wurde es automatisch langsam heller im Raum. Er ging ins Badezimmer und stieg unter die Dusche, seifte sich gründlich ab und genoss das Wasser, das ihm in genau der richtigen Temperatur über den Kopf plätscherte. Ein flauschiges Handtuch und der Tag konnte beginnen. Er würde lang werden.

Notwendigkeit eines Identitäts-Managers

Nach dem Frühstück ging Björn aus dem Haus, musste allerdings noch einmal schnell umkehren, weil er seinen PIMCO (Personal Identity Manager, Communicator and Organiser) beim Anziehen der Schuhe auf dem Treppenabsatz hatte liegen lassen. Ohne den PIMCO, ein kleines handliches Gerät, würde er den Tag über ziemlich wenig zu Wege bringen geschweige denn überhaupt zur Arbeit gelangen. Denn die öffentlichen Verkehrsmittel ließen sich nur deshalb so reibungslos nutzen, weil man keine einzelnen Fahrscheine mehr lösen musste, sondern der PIMCO mit den in den Wagen der Stadtbahn aufgestellten Ter-

Delegation an Softwareagenten

minals kommunizierte. Am Ende des Monats wurde aus den Daten über die vorgenommene Nutzung des ÖPNV automatisch der günstigste Tarif für Björn errechnet und von seinem Konto abgebucht.

Bewegungsprofile

Eine Stunde dauerte die Fahrt zur Arbeit. Genug Zeit, um unterwegs noch einmal alles durchzugehen. Heute fuhr er erster Klasse; sein PIMCO verband sich mit dem an seinem Platz bereitstehenden Bildschirm und der Tastatur und stellte eine weitere Verbindung zum Firmenserver her.

Allgegenwärtige Internetkonnektivität

Aus dem Fenster hatte Björn lange Zeit einen guten Blick auf die parallel zum Zug verlaufende Autobahn. Der Verkehr war dicht, aber gleichmäßig fließend, ohne Staus. Dies war hauptsächlich der automatischen Geschwindigkeitsbegrenzung zu verdanken, die auch die Zahl der Unfälle in den letzten Jahren deutlich reduziert hatte. Abhängig von den Wetterbedingungen und dem Verkehrsaufkommen wurden die Fahrzeuge anhand von ausgeklügelten Algorithmen flexibel abgebremst oder beschleunigt, um den Gesamtfluss des Verkehrs zu optimieren. Kreuzungen zum Beispiel kamen schon seit Jahren ohne Ampeln aus, da die sich kreuzenden Verkehrsströme koordiniert miteinander verwoben wurden. Niemand musste mehr anhalten und warten.

Übergang von individueller zu koordinierter Steuerung

Das wurde durch zahllose Sensoren und spontane Kommunikation zwischen Autos untereinander, mit Service-Anbietern im Internet und auch mit den intelligenten, dynamischen Straßenschildern erreicht, deren optische Anzeigen eigentlich nur noch für die „Oldtimer“ unter den Autos interessant waren, die aber ab nächstem Jahr gar nicht mehr zugelassen sein würden. Die neueren Fahrzeuggenerationen waren einfach sicherer und verfügten über bessere Selbstwartungsfunktionen.

Zentral organisierte und spontane Ad-hoc-Netze

Eigentlich musste Björn gar nicht mehr jeden Tag zur Arbeit fahren,

sondern konnte sich von seiner Wohnung aus so wie jetzt in der Bahn virtuell ins System seiner Firma einklinken und so arbeiten und mit den Kollegen kommunizieren, als sei er im Büro. Die asiatischen Geschäftspartner, die sich für heute angesagt hatten, waren aber nicht extra den weiten Weg gereist, um dann nur per Videokonferenz mit ihm zu reden – dies wäre auch aus Asien kein Problem gewesen. Sie wollten sich einen persönlichen Eindruck von ihm verschaffen und – sofern der Eindruck kein schlechter wäre – bei der Gelegenheit ein paar Verträge unterzeichnen.

VPN als Teil des Arbeitsalltags

Einen guten Eindruck wollte Björn gern hinterlassen. Deshalb ging er nicht nur die Vertragsentwürfe erneut durch, sondern arbeitete sich die letzte halbe Stunde der Fahrt durch einen Schnellkurs zu den kulturellen Besonderheiten seiner Gäste, den sein PIMCO ihm auf Basis seines Lernprofils aus dem Internet herausgesucht hatte. Und auch ein paar Worte in der fremden Sprache durften nicht fehlen – zumindest kam seine Begrüßung – ohne den automatischen Übersetzer, der sich dann aber um den Rest der Konversation kümmerte – gut an, wie sich beim Eintreffen der asiatischen Delegation zeigte.

E-Learning, angepasst an spezielle Anforderung und Profil des Lernenden

Ein Rundgang durch die Firma, durch Entwicklung und Produktion, begleitet von ein wenig Smalltalk, schaffte schnell eine angenehme Atmosphäre. Die PIMCOs der Besucher waren im Firmensystem registriert worden und erlaubten ihnen nun den Zutritt zu den sonst abgesicherten Unternehmensbereichen. Während seine Gäste sich vom Produktionsleiter das neue Verfahren erläutern ließen, mit dem die Kostenvorteile der Serienproduktion mit dem Kundenwunsch nach einer Maßanfertigung zusammen gebracht wurden, trat Björn kurz beiseite, um seiner Freundin die traurige Videobotschaft aufzunehmen, dass er es heute Abend leider doch nicht zu ihr schaffen würde. Über seinen PIMCO buchte er zwei digitale Theaterkarten für den nächsten Tag. Botschaft und Karten würde sie sehen können, sobald sie in ihrem PIMCO den privaten Modus wieder aktivierte. Da sie bei der Arbeit ungern gestört wurde, sorgte ihr PIMCO dafür, dass sie nur geschäftlich notwendige Kontakte erreichten.

Zutrittskontrolle, auch Arbeitszeiterfassung und ggf. Tätigkeitsprotokollierung

Adaptive Produktionsverfahren

Erreichbarkeitsmanagement

Björn musste sich morgen unbedingt auch bei seinem Team bedanken, das ihn bei den Vorbereitungen des Besuchs der Delegation aus Asien unterstützt hatte, denn neben den geplanten Verträgen wurde auch noch eine Vorvereinbarung für eine langjährige Kooperation unterzeichnet. Offensichtlich hatten er und seine Firma einen sehr guten Eindruck hinterlassen. Nicht zuletzt das abendliche Essen, das sich an den geschmacklichen Vorlieben der asiatischen Gäste orientierte, hatte dazu beigetragen. Sein Assistent hatte die Informationen aus den Protokolldaten der Hotels und Restaurants gewonnen, die in den letzten Wochen von der Delegation besucht worden waren. Es war nicht billig gewesen, an diese eigentlich unzugänglichen Daten über die (nicht nur kulinarischen) Vorlieben und Gewohnheiten der Gäste heranzukommen, aber es hatte sich gelohnt.

Profil über private Vorlieben von Geschäftspartnern

Data Mining zu persönlichen Vorlieben

Die Rückfahrt nach Hause lohnte sich für Björn heute nicht mehr, dazu war es viel zu spät geworden. Als der sinnvolle Zeitpunkt für eine Rückkehr verstrichen war, hatte sein PIMCO ein Zimmer in einem Hotel in der Nähe gebucht und Björns Profil übermittelt. Als er dort eintraf, hatte der Raum das für ihn ideale Gefüge aus Temperatur, Luftfeuchtigkeit und Beleuchtung. Wenigstens wurden die Überstunden gleich automatisch erfasst. Mal schauen, ob er sie abbummeln oder sich ausbezahlen lassen würde.

Planungsinformation, Vernetzung mit externen Datenbeständen, persönlichen Profildaten

Björn sank erstmal in den Sessel und aktivierte den Großbildschirm. Sein PIMCO verband sich mit diesem und dem Server seines Medien-Providers, lud dort den am Vorabend begonnenen Spielfilm sowie zwei Folgen von Björns Lieblingsserie herunter und begann das Abspielen des Spielfilms an der Stelle, an der Björn gestern eingeschlafen war. Heute schaffte er immerhin noch die erste der beiden Serienfolgen.

Vernetzter Medienkonsum

4.3 Szenario 2: Ferien

Endlich Ferien. Anneke stand aus ihrem Bett auf und trat ans Fenster, dessen Jalousie sich langsam öffnete. Der Blick in den Garten mit den bunt blühenden Blumen und dem frischen Grün der Bäume und Sträucher hatte zusammen mit der Vorstellung, sich in den nächsten Wochen einfach nur entspannen zu können, etwas ungemein Belebendes. Schnell unter die Dusche und dann runter auf die Terrasse zum Frühstück, wo bereits ihre Eltern saßen. Ihr großer Bruder Tom schlief na-

türlich noch. Er hatte die letzte Nacht auf einer Party in den Ferienbeginn hineingefeiert.

Energieversorgung kabelfrei

„Weißt Du, Sophie, ich dachte wir schauen heute Nachmittag noch mal bei meiner Mutter rein," sagte Carsten, Annekes Vater, gerade, als die 15-Jährige dazu kam. Auf dem Tisch stand der Toaster, der aus der Tischplatte induktiv mit Strom versorgt wurde, so dass keine Kabel mehr umständlich in den Garten verlegt werden mussten. Der Tisch wiederum bekam seine Energie nach dem gleichen Prinzip aus im Terrassenboden verlegten Leitungen. Anneke legte zwei Scheiben Vollkorntoast ein. „Goldbraun" sagte sie zum Toaster und beobachtete, wie die Brotscheiben in seinem Innern verschwanden.

Sprachsteuerung (HCI)

Planungsinformation, Vernetzung mit externen Datenbeständen, Data Mining

Nachmittags wollte die Familie zu ihrem Ferienhaus auf einer Mittelmeerinsel aufbrechen. Daher galt es, noch schnell die letzten Vorbereitungen zu treffen. „Sind eure Koffer schon gepackt?" fragte Sophie. „Ich weiß nicht, wie es bei Tom aussieht, aber bei mir ist alles vorbereitet." Alles vorbereitet – das hieß, dass sie der Kleiderverwaltung des Haus-Systems kurz mitgeteilt hatte, wie lange sie wohin verreisen wollte. Das System hatte sich die Wetterdaten und -prognosen für die Insel heruntergeladen und aus den Protokollen über die Tragehäufigkeit von Annekes Kleidung ihre passenden Lieblingsklamotten für den Urlaub zusammengestellt. Im Moment wurden diese gerade aus dem Wäschespeicher herausgesucht und über das Verteilsystem in ihr Zimmer gebracht, wo sie alles einmal durchschauen und in den Koffer packen würde.

Automatisierung der Wohnumgebung

Virtualisierung der Realität

Häufige Übermittlung von persönlichen Krankheitsdaten und sensiblen Messwerten

Nach dem Frühstück – Tom war noch immer nicht aufgestanden – fuhren Carsten und Sophie ins betreute Wohnheim, in dem Carstens Mutter seit einem halben Jahr lebte. Es ging ihr nach einem Schlaganfall nicht besonders gut und Carsten machte sich durchaus Sorgen um sie. Früher wäre sie in die Ferien mitgefahren, aber das ging jetzt nicht mehr. Carsten aktivierte die Bildwand in ihrem Zimmer und stellte eine Verbindung zum Ferienhaus her. Über ein einfaches Stimmkommando konnte seine Mutter sich nun Bilder und Geräusche, durch einen Aromasynthesizer sogar die Gerüche des Ferienhauses in ihr Zimmer holen. Umgekehrt konnte die Familie sich ständig über ihren Gesundheitszustand informieren und notfalls mit dem Ärzteteam beraten. Obwohl man so ganz einfach „beieinander" sein konnte, legte Carsten großen Wert darauf, vor längeren Abwesenheiten persönlich bei der älteren Dame vorstellig zu werden.

Zuhause angekommen sorgte Sophie zunächst dafür, dass Tom endlich aufstand, indem sie seinem Zimmer viel Licht und laute Musik verordnete – im Zweifel stellte das System ihre Anweisungen über die von Tom, so hatten die Eltern es konfiguriert. Als sie schon kurz darauf die Toilettenspülung hörte, konnte sie ein Lächeln nicht unterdrücken.

Kontrollverlust über die eigene UC-Umgebung

Während Tom nun ebenfalls unter die Dusche stieg, wollte Sophie noch ein letztes Mal alles überprüfen. „Computer, wie ist der Systemstatus?“ fragte sie. Auf der Wand zur Rechten ihres Sessels erschien ein dreidimensionaler Plan von Haus und Grundstück. Nach und nach wurden alle darin enthaltenen Systeme grünlich eingefärbt, und eine freundliche Stimme sagte: „Alle Systeme erfüllen die vorgesehene Funktion. Es wurden keine Probleme gefunden.“ Beruhigt lehnte Sophie sich zurück – in den letzten Wochen hatte es einmal ein paar Fehler bei den Feuchtigkeitssensoren im Salatbeet gegeben, das daraufhin von der Bewässerung komplett unter Wasser gesetzt worden war. Dies wiederum hatte einen Kurzschluss in einem Bewegungssensor verursacht, der Teil der Alarmanlage war. Der Fehler war im Nachhinein schnell gefunden und behoben, hatte aber doch zunächst für einige Aufregung gesorgt.

Fehler in Programmen, physische Folgeschäden

Inzwischen hatte Carsten angefangen, das Gepäck im Kofferraum seines Wagens zu verstauen, nachdem sogar Tom seinen Koffer noch rechtzeitig abgeliefert hatte. Beim Mittagessen war er dann auch mit dabei und fing sich mahnende Blicke seiner Eltern und ein breites Grinsen seiner Schwester ein, als das Haussystem ihn darauf hinwies, dass er aufgrund des Defizits an Vitaminen und Mineralien in seinem Körper statt einer Cola lieber einen Vitamin-Cocktail zu sich nehmen sollte. Allen war klar, dass dieses Defizit wohl mit dem Genuss alkoholischer Getränke am Vorabend in Zusammenhang stand.

Überwachung von Körperfunktionen, Empfehlungen und Folgepflichten

Soziale Implikation

Nachdem Anneke (die heute an der Reihe war) das Geschirr in den Spüler gestellt hatte, zog die Familie sich um, denn gleich sollte es losgehen. Als alle im Auto waren, fuhr Carsten los. Nach etwa 10 Minuten waren sie an der nächsten Autobahnauffahrt angekommen. Carsten beschleunigte noch etwas, lehnte sich dann zurück und genoss den Blick durchs Panoramafenster im Dach. Der Autopilot hatte die Steuerung übernommen und Carsten wollte noch ein kurzes Nickerchen einlegen. Tom suchte sich hinten inzwischen über das Internet ein Buch heraus, dass er während der Fahrt lesen wollte, und ließ es sich auf seinen PDA übertragen.

Abgabe von Kontrolle

Nach ca. einer Stunde waren sie am Flughafen angekommen und fuhren am Drive-by-Check-in-Schalter vor. Dort stiegen sie aus, gaben ihr Gepäck ab und sahen zu, wie ihr Wagen vom Flughafensystem ins Parkhaus weitergefahren wurde. „Wieder reif für die Insel?“ fragte der Beamte am Eingang zu den Laufbändern, die sie zu ihrem Flieger bringen würden. Nachdem die Familie sich per Iris-Scan identifiziert hatte, konnte er anhand ihres Reiseprofils auf seinem Bildschirm sehen, dass sie regelmäßig den gleichen Ort aufsuchten.

Reiseprofil bei Sicherheitsbehörden

Biometrische Identifikation von Reisenden

Endlich im Flugzeug sitzend aktivierte Tom gleich per Handbewegung den Bildschirm in der Lehne des Sitzes vor ihm. Er wählte den Blick über die Kamera im Boden des Fliegers, um beim Start ja nichts zu verpassen. Anneke neben ihm fand das nicht besonders spannend und setzte stattdessen ihre Sonnenbrille mit eingebautem Display und Surround-Kopfhörern im Bügel auf. Sie wollte sich mit einem romantischen Film auf den Urlaub einstimmen. Sophie blätterte in einer Zeitschrift und Carsten schnarchte schon wieder ganz leise. Sophie lächelte. Sie wusste, von wem ihr Sohn die Langschläfer-Gene hatte.

Allgegenwärtigkeit von Überwachungskameras

4.4 Szenario 3: Einkaufserlebnisse der ubiquitären Art

Es war Samstag Nachmittag. Alice hatte endlich mal wieder richtig Zeit zum Shoppen. Ein besonderer Spaß waren die individuellen Touren, die sie in den Mark Weiser Arkaden – Berlins größter Shopping Mall – nutzen konnte. Auf Basis ihrer Kundenkarte, mit der sie regelmäßig dort einkaufte, wurden ihr individuelle Angebote gemacht, wenn sie diese wünschte. Normalerweise hatte sie keine Zeit, ihre schnellen Einkäufe nach der Arbeit auch noch durch die persönlichen Vorschläge an Regal- und Schaufensterbildschirmen unterbrechen zu lassen. Aber heute hatte sie mal richtig Lust darauf, sich inspirieren zu lassen. Sie ging dazu durch die rechte Eingangstür, ein separater Eingang für alle diejenigen, die Werbung wünschen – ginge sie durch die linken, größeren Türen, so wäre sie, wie auch früher immer, unerkannt und anonym in der Mall.

Kundenkarte mit hinterlegtem Konsumprofil

Kundenberatung / Werbung auf Basis von Konsumprofilen

Selbstbestimmungsmöglichkeiten

Nach Durchlaufen wurde sie aufgefordert, eine PIN einzugeben, die zu ihrer persönlichen Kundenkarte gehörte. Die Mall bekam so die Erlaubnis, ihre Kundenkartendaten via Funk auszulesen und ihr auf Basis der hier gespeicherten persönlichen Präferenzen und früheren Einkäufe Empfehlungen zu schicken. Bei Abschluss des Kundenkartenvertrags hatte Alice damals zuge-

Sicherheitsproblem PIN-Länge

Leichte Abhörbarkeit

„Push“ benötigt Einwilligung, (hier allerdings nur einmalig)

stimmt, auch Rabattcoupons via SMS zu empfangen, wenn sie mittags in die Mall ging. So etwas war praktisch, denn manchmal konnte sie so von besonderen Menüangeboten profitieren.

Profildaten

Ein besonderer Service der Mall war auch, dass Sie zwischen zwei eigens für sie zusammengestellten Touren auswählen konnte, an deren Wegesrand besondere Angebote der Shops auf sie warteten. Dies erlaubte ihr, bei all den Vorschlägen trotzdem im Schnitt nicht mehr als zwei Stunden an einem solchen Nachmittag in der Mall zu verbringen. Dies war die von ihr im Kundenkartenvertrag spezifizierte Maximalzeit. Die Mall, das wusste sie, sorgte für eine sinnvolle Selektion der Angebote und hatte den Ruf, sich mehr an Kundenpräferenzen und früheren Einkäufen für die Beratung zu spezialisieren als an den großen Marken. Werbung der Megaunternehmen wie NiceTry oder Geppi sah man ohnehin überall. Aber bei solch einer Tour mochte man auch schon mal etwas ganz Neues entdecken. Als Betriebswirtin wußte Alice, dass sie damit auch kleine und unbekanntere Geschäfte und Marken förderte.

Selbststeuerung von Angeboten

Ein weiterer positiver Punkt, den sie immer wieder hervorhob, wenn sie zu dem Mall-Service befragt wurde, ist der Umgang des Betreibers mit ihren persönlichen Daten. Bis vor kurzem hatte Alice die Kundenkarte genutzt, ohne je ihren Namen und ihre Anschrift anzugeben. Sie war der Mall und den Shops einfach nur als ‚Alice' bekannt und davon gab es in Berlin eine Menge. Trotzdem waren die Angebote sehr gut, denn sie hatte vor dem Hintergrund dieser pseudnomymen Gestaltung des Programms keine Bedenken, mehr Präferenzen von sich im Kundenkartenformular einzutragen, als sie dies normalerweise bei anderen Programmen machen würde.

Pseudonymisierung

Einsicht in das eigene Profil mit Änderungsmöglichkeit

Da die Angebote ihr in letzter Zeit jedoch so viel Spaß gemacht hatten, hatte sie im letzten Monat einen besonderen Kundenkartenvertrag mit der Mark Weiser Arkaden GmbH abgeschlossen. Diese durfte ihr nun auch wöchentlich eine individuelle Angebotspost nach Hause schicken. Über ein Online-Portal konnte sie auf der Webseite der GmbH jederzeit sehen, welche Einkäufe in ihr Profil mit eingingen. Sie konnte festlegen, ändern und löschen, für welche Produkte und Branchen sie sich interessierte (bei ihr waren es Kleidung und Blumen). Auch ihre Einkäufe konnte sie gezielt löschen. Davon hatte sie sogar schon mal Gebrauch gemacht. Die GmbH hat ihr vertraglich zugesichert, dass ihre Daten nur bei der GmbH selbst verbleiben und auch mit der Muttergesellschaft, der Ray Kurzweil Inc., nicht geteilt

Kontrolle und Durchsetzung von Betroffenenvorgaben

Keine spezifischen Bewegungsprofile, keine Verkettung von Datenbanken / Konsumprofilen

Komplexität von Betroffeneninformation

Betroffenenpräferenzen

wurden. Auch einzelne Shops und Handelsmarken erhielten keine Einsicht in Alices persönliches Profil, geschweige denn ihre Anschrift. Sie wussten nur jeweils, was das Pseudonym ‚Alice' bei ihnen direkt gekauft hatte und konnten allgemeine Bewegungsprofile bei der GmbH erfragen, wie sich Besucher generell durch die Mall bewegten. Ein Grund für Alice, diesen Vertrag abzuschließen, war, dass Sie wirklich zu 100% verstanden hatte, was mit ihren Daten passierte. Statt der üblichen zehn Seiten an Kleingedrucktem hatte die GmbH ihr einfach nur einen 10-Punkte Plan geschickt mit der Aussage, was mit ihren Daten gemacht wurde und was nicht. Diese Transparenz hatte ihr Vertrauen gewonnen.

Automatisierte Beratung anhand von Profildaten

Nachdem ihr der intelligente Spiegel bei Bonotti empfohlen hatte, dass rot dieses Jahr „in" sei und zu den Blue Jeans passe, die sie letzten Winter gekauft hatte, war Alice nun guter Laune. Früher war sie sich gerade bei Farben immer unsicher gewesen, aber der intelligente Spiegel kannte ja ihren Teint und ihre schwarze Haarfarbe. Was für ein Glück, dass es heute solche stilsicheren Services gab. Erst kürzlich hatte sie gelesen, dass das Haus Carl Zeltlager bei M & H die Spiegelberatung machte. Das war ein echter Mehrwert. Zufrieden ging sie zum Thai, der ihr per SMS einen Coupon zugeschickt hatte. Das Essen war vorzüglich. Sie überlegte, ob sie den Thai vielleicht doch in ihr Präferenzprofil aufnehmen sollte, damit es in Zukunft häufiger Coupons gäbe.

4.5 Szenario 4: Verbrechen der ferneren Zukunft

Ferngesteuerte Fehlfunktionen

Physischer Schaden durch Cyberangriffe

Immer diese verregneten Nachmittage, und natürlich, wieder ein Anschlag eines UC-Terroristen auf eine Einkaufsmeile. Und natürlich: Ich als stellvertretender Ermittlungsassistent zweiten Grades des Amts für Ubiquitäre Sicherheit musste persönlich an den Tatort, um inmitten des Chaos nach Hinweisen zu suchen, die es wahrscheinlich gar nicht gab. UC-Straftäter hinterlassen keine physischen Spuren, sie kommen aus dem Nirgendwo des Netzes. Sie nutzen die allgegenwärtige Sensorik und spionieren ihre Ziele aus der Ferne aus, und mithilfe manipulierter Daten und vorgespiegelter Kontexte veranlassen sie Aktuatoren zu Aktionen, die Menschen schaden.

Sicherungssysteme sind gleichermaßen unsicher

So auch in diesem Fall: Hier schien jemand das automatische Küchensystem eines beliebten Fast-Food-Restaurants in den Ray-Kurzweil-Arkaden aus der Ferne übernommen zu haben. Nicht nur, dass sämtliche Speisen durch gefälschte Kochre-

zepte ungenießbar waren, sie waren auch giftig. Das redundante Safety-Subsystem der UbiKüche benutzte heute aufgrund von außerplanmäßigen Wartungsarbeiten (wer hatte die veranlasst?) denselben MAN-Uplink wie das Hauptsystem. Da der Patchstand des Systems einige Minuten zu alt war, konnte vermutlich ein typischer Search&Break-Softwareagent innerhalb von Sekunden eindringen und sich mithilfe seiner flexiblen Adaptivität zu einem Kontrollagenten dieses spezifischen UbiKüchentyps verwandeln. Na ja, nun lagen dreißig Gäste in den HealthMobiles.

Personenschäden

Die Küche war ein einziges Trümmerfeld, alle Kochaktuatoren und Siedestrahler waren in einem finalen Akt von UbiVandalismus weit außerhalb ihrer üblichen Spezifikationen benutzt worden und hatten nach Abschaltung der Sicherheitssysteme mit der Zerstörung des Raumes begonnen.

Sachschäden

Ich begann meine Ermittlungen in der InfoFreezeBubble, die die Beamten der Kriminalpolizei in einem Radius von einem Kilometer errichtet hatten, die mittels des staatlichen Masterkeys alle legalen Sensorsysteme samt ihren Datenbanken den Ermittlern unterstellte.

Globale Kontrolle privater UC-Systeme für Staatsorgane

Zunächst überprüfte ich, ob sich auch alle ca. fünf Millionen Sensorsysteme in diesem Radius – inklusive aller persönlichen BodyCams von Privatpersonen, die sich heutzutage des Öfteren ein modisches drittes Auge in die Stirn implantieren lassen, sich aber ebenfalls an die UC-TK-Richtlinie halten müssen. Diese sieht eine mindestens zehnjährige – ich muss leider sagen, nur aggregierte – Datenspeicherung zur Verbrechensbekämpfung vor. Aus meiner praktischen Erfahrung legte ich aber wenig Hoffnung in diesen Datenozean, da die meisten der smarteren Terroristen üblicherweise aus weiter Ferne über diverse Datentunnel agierten. Aber die UC-TK-Richtlinie entstand zu Wahlkampfzeiten nach einem größeren Anschlag, und wenige Politiker trauten sich, für ihre Rücknahme zu votieren.

Videoüberwachung durch jedermann

Vorratsdatenspeicherung

Technischer Fortschritt und starre Gesetze

Schwierige Rückverfolgbarkeit

Kosten der Strafverfolgung

Und nun gehörte dieser Datenozean in unseren Ermittlungsalltag. Zunächst mietete mein PoliSec-Agent genügend große Speicher- und Auswertungskapazitäten bei kommerziellen Grid-Anbietern an, die in einer „Reverse Auction“ darum wetteiferten, mir als Ermittler den günstigsten Preis zu bieten. Ja, diese Privatisierung der öffentlichen Computerressourcen hatte die Staatsverschuldung etwas geringer anwachsen lassen. Leider ließen die Datenmassen und ihre Verschiebung über drahtlose Systeme kaum Verschlüsselungsmaßnahmen zu; aber die Unternehmen

Privatisierung von Rechenleistung und Datenbanken

Datenunsicherheit

hatten sich ja freiwillig verpflichtet, die Daten nach Ende der Ermittlungen wieder von ihren Systemen zu löschen. Und im Augenblick sammelte ich auch nur Daten von heute. Die Langzeitauswertung würde dann wiederum an private Spezialfirmen ausgelagert.

Outsourcing staatlicher Gewalt

Meine Data Mining-Vorliebe, auf die ich besonders stolz bin, ist die Suche nach Herzschlagfrequenzen außerhalb der üblichen Normen. Wie oft habe ich bei meinen Ermittlungen zwar nicht den Hauptfall lösen können, aber doch dutzende von kleineren Delikten oder Stadtraum-Nutzungsverstößen an die lokale Polizeibehörde übergeben können. Folgt man nämlich dem erregten Herzschlag und aktiviert in einigem Umkreis die Kameras, so bekommt man einiges an Illegalem zu sehen, das können Sie mir glauben.

Data Mining auf Basis medizinischer Echtzeitdaten

Kollateralfunde bei Ermittlungen

Doch heute wollten nicht einmal die Feuchtigkeitssensoren auf den zehntausenden von Türgriffen mir schweißnasse Verbrecherhände melden – schnell erwiesen sich alle Verdachtsfälle durch Liveüberwachung als Fehlalarme. Auch die Pattern-Matching-Algorithmen gaben keine verdächtigen Muster bei den Bewegungen der weltweit eindeutigen RFID-Tags, die seit 2017 bei der Geburt implantiert werden. Jugendliche lokale Straftäter, die gerne mit selbst gebastelten GangstaBlokka-Agents UC-Systeme verwirren und sabotieren, schloss ich deshalb für den Anschlag heute aus.

Überwachung durch flächendeckende Sensorik, zentrale Auswertung von Datenbeständen

Eindeutiges Personenkennzeichen im Körper

Einfache Sabotagemittel

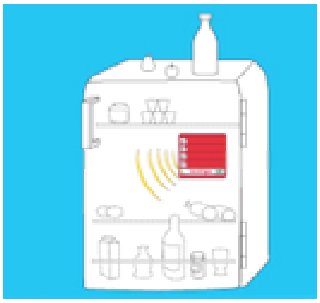
Es war wirklich, wie vermutet, eine Aktion aus dem Nirgendwo. Aber dank des genetischen Profilings, das für Terroristen und Hacker typische Kombinationen von Genen automatisch meldete, woraufhin verstärkte lebenslange UbiSurveillance angeordnet wird, werden wir in einigen Jahrzehnten hoffentlich auch damit keine Probleme mehr haben.

Maßnahmen auf Prognose- und Wahrscheinlichkeitsbasis

Interpretation menschlichen Verhaltens durch Technik

Mit einem Seufzen schloss ich alle Gridverbindungen und genehmigte mir bei einem der letzten Straßenverkäufer einen von Menschenhand gemixten Vitamindrink. Sicher ist sicher.

4.6 Szenario 5: Mein neuer Kühlschrank



Bei meinem morgendlichen Aufwachritual in unserer neuen automatisierten Küche schlich sich ein roter Farbton über die Schwelle meiner noch recht begrenzten Wahrnehmung.

Aha, der Kühlschrank – seine sonst so makellos weiße Farbe wurde nun von einem farbigen Bildschirmhintergrund auf seinem Touch-Pad geschmückt. Er will mir doch etwas mitteilen, dachte ich. Mein etwas müdes und grübelndes Starren fasste die diensteifrige „Kühlschrankintelligenz“ nach einiger Zeit als Aufforderung auf, mich mit mehr Informationen auf dem Bildschirm zu bedienen.

Usability-Probleme

Autonomes Safety-System

Soso, es hatte ein Problem bei der nächtlichen automatischen Inventur und Nachbestellung von Waren gegeben. Meine noch etwas unkoordinierten Finger trafen nun aus Versehen die Fläche für „Technische Details“, und was ich las überforderte mich doch ein wenig:

Probleme bei der automatischen Interpretation der Realität

`2014-05-21-04:00:03 [Health Protection Subsystem] Anonymisierte VPN Verbindung zum P2P HealthNet aufgebaut. Datenauffrischung 4192 KB. Signatur: gültig.`

Verschlüsselte und anonymisierte Verbindung zu Servern mit Verträglichkeitsdaten

`2014-05-21-04:00:05 [Health Protection Subsystem] Automatische Bestellung des Hauptsystems bei Agrarproduktagent (ID F6C312) wurde gestoppt. Grund: Exaktes Produkt („Vollmilch“, Marke: „Kuhstolz“, Prod.-ID ECDFF234) augenblicklich nicht verfügbar, angebotenes Substitut („Vollmilch“, Marke: „Almenglück“, Prod.-ID ECDF2FE9) verwendet unbekannte Ontologie bei der Beschreibung (V 327.892+).`

Update der Kühlschrankintelligenz

`2014-05-21-04:00:08 [Main System] Ontologie-Update (V 327.902) erfolgreich. Neuaushandlung der Bestellung mit Agrarproduktagent (ID F6C312) erfolgreich.`

`2014-05-21-04:00:10 [Health Protection Subsystem] Alternative entspricht lokalem Gesundheitsprofil. Bestellung erlaubt. Nutzerbefragung eingeleitet.`

Einkaufskontrolle durch lokal gespeicherte Gesundheitsprofile

Ganz schnell wanderte mein Finger auf das Feld „Erklärung“. Hier sprach nun mein Kühlschrank als Gesamtperson:

HCI-Design: Leicht zugängige und aussagekräftige Hilfsfunktionen

`Lieber Nutzer, guten Morgen! Deine Lieblingsmilch der Marke Kuhstolz ist zurzeit nicht in der von Dir benannten Preisspanne und Geschwindigkeit verfügbar. Meine Bestellung erfolgte nun für ein ähnliches Produkt. Mein Gesundheitscheck ergab, dass sich die Bestandteile nicht wesentlich von Deiner Lieblingsmarke unterscheiden.`

Auskunftsmöglichkeit, Transparenz

`Bitte teile mir doch durch Druck auf den [OK] Knopf oder Kopfnicken mit, ob diese Alternative auch in Zukunft infrage kommt.`

ID-Management im täglichen Gebrauch

Mit [NEIN] machst Du die Bestellung rückgängig.

Mit [VERLAUF] kannst Du die getroffenen Entscheidungen auch später ändern oder widerrufen.

Einfache Interaktion

[PRIVAT] führt in ein Menü, wo Du alle über Dich gespeicherten Daten ansehen, bearbeiten und Berechtigungen verteilen kannst. Auf Wunsch kann ich dies auch mit Deinem Privacy-Assistenten aushandeln.

Selbstbestimmung und Kontrolle automatisierter Prozesse bei Abweichungen von der Norm. Unterstützung der Entscheidungsfindung

Werde ich später entscheiden, dachte ich. Nach dem ersten Kaffee ließ ich mir aus Neugier von meinem persönlichen „Privacy-Assistenten“, den ich in meiner Armbanduhr integriert hatte, einen kurzen Statusbericht geben. Nebenbei bemerkt, ich liebäugele schon mit der Assistentenvariante PrivacyRokka (einer sehr massiven Gürtelschnalle), während meine Nachbarin, ein echter NeoGeek, ihren Assistenten zusammen mit neuen Antennen in ihre leuchtenden Haarnadeln integrieren ließ – sie beschwerte sich danach nie wieder über mangelnde Konnektivität ihres Body-Area Networks. Aber manchmal hatte sie leider kein temporäres Interface in ihrer Nähe zur Verfügung – die kann man sich üblicherweise für eine bestimmte Zeit leihen, um sicher und ohne hinterlassene Datenspuren mit der eigenen oder anderen UC-Umgebungen zu kommunizieren. Das Leben ist voll von Kompromissen.

Alltägliche Vernetzungsprobleme

Anonymer Netzzugang

Kontrolle eigener Datenspuren / Profilbildung in Hintergrundsystemen / Weitergabe von Daten

Die Episode mit dem Kühlschrank ergab auf meine Nachfrage eine ganze Menge Details, insbesondere wo und welche Informationen über mich übertragen worden waren, um neue Waren zu bestellen, und wie lange die Lebensdauer der Daten war. Da ich die Schritte des Lieferanten bereits gehört hatte, der meine Box neben der Tür aufgefüllt hatte, und seine Lieferungen üblicherweise äußerst korrekt sind, drückte ich den grünen „Datenspuren Löschen“-Knopf des Privacy-Assistenten.

Kontrolle über eigene Daten

Das Pseudonym auf dem Chip an der Tüte, der nur bei Berührung auslesbar ist, ist alles, was ich für etwaige Reklamationen benötige – Details wie Name, Kontoverbindung und Adresse würden von meinen Softwareagenten neu ausgehandelt werden. Datenschutz-Reputation von Händlern, sowohl gewährleistet durch staatliche und private automatische Audits als auch durch Käuferbewertungen, ist ja inzwischen zu einem wichtigen Faktor beim automatischen Aushandeln von Geschäften geworden, und so vertraue ich den Händlern, die mein Softwareagent für mich ausgewählt hat.

Sicherung durch Auslesbarkeit nur bei physischem Kontakt

Kontrolle von Datenverarbeitern

Reputation als Vertrauensmerkmal

Datenschutz als Wettbewerbsvorteil

Ach ja, seit den großen Privacyskandalen und der Aufdeckung

von Industriespionage in ungeheurem Ausmaß ist es gesellschaftlich und bei vielen Konzernen durchaus akzeptabel, auch während der Arbeitszeit einen kleinen Teil der Aufmerksamkeit dem Schutz sowohl der eigenen Privatsphäre als auch der des Unternehmens - als virtueller Person - zu widmen. Die gelungene Benutzerführung meines Agenten beschleunigt diese neuen „Rituale“ ungemein.

Bewusstsein für IT-Sicherheit und Privatsphäre

Benutzerfreundliche Privacy Enhancing Technologies (PETs)

4.7 Szenario 6: Fliegen mit Herz … und Ubiquitous Computing

Endlich. Die Mitarbeiterin am Gate eröffnete das Boarding. Zunächst brachten Mitarbeiter des Flughafens einen älteren Herrn mit dem Rollstuhl in die Kabine, dann begann der Rest der Passagiere, um den besten Platz in der Boardingschlange zu kämpfen, als gäbe es keine Platzreservierungen.

Nachdem wir unseren Fingerabdruck an einem Scanner hinterlassen und uns so identifiziert hatten, bestiegen wir das Flugzeug und rollten zügig zum Start. Wir stiegen schnell mit Kurs gen Ostsee. Über Schleswig-Holstein wurde es turbulent. Die Achterbahnfahrt begann mit einem riesigen Luftloch. Lose Gegenstände begaben sich im allgemeinen Aufschrei der Passagiere gen Kabinendecke. Die Maschine wurde mal auf die eine, dann auf die andere Seite geworfen, während das arbeitende Material des Rumpfes wenig vertrauenerweckende Geräusche von sich gab.

Biometrische Zugangskontrollen

Für den älteren Herrn mit Rollstuhl, der zwei Reihen vor mir saß, war dies offensichtlich zu viel. Typische Anzeichen einer Herzschwäche stellten sich ein. Nachdem das Kabinenpersonal keinen Arzt unter den Passagieren finden konnte, brachten sie den mobilen NotfallMedicus zum Einsatz. Dieses Gerät wurde von einer Stewardess mit Basisinformationen wie dem Gewicht und dem Alter des Patienten gefüttert und überprüfte selbst mittels verschiedener Sensoren relevante Vitalfunktionen des Patienten. Die automatische Auswertung dieser Informationen untermauerte, dass ein unregelmäßiger Herzrythmus mit Aussetzern als Diagnose wahrscheinlich war. Daher erlaubte der Medicus der Stewardess die Freigabe eines wohldosierten Stromstosses, der das Herz des Mannes wieder in den richtigen Rhythmus bringen sollte. Dies gelang offensichtlich, doch stellten sich immer wieder kleinere Rückfälle ein.

Automatisierte Verknüpfung von Notfallstrukturen

Kontrolle menschlicher Handlungen in Stresssituationen

So informierte uns der Flugkapitän, dass wir unseren Flug

aufgrund eines medizinischen Notfalls unterbrechen würden. Er hatte eben das GDIS (Global Distress Information System) aktiviert. Seit einigen Jahren waren Flugzeuge und andere Verkehrsmittel über Satelliten an das Internet angebunden. GDIS ermittelte mit Hilfe des europäischen GALILEO-Systems hochpräzise den Flugzeugort sowie welche Flughäfen in der Nähe für eine Landung dieses Flugzeugstyps geeignet waren, welche am schnellsten zu erreichen waren und ob die Wetterbedingungen und der Status des Flughafens eine Landung zuließen.

Vernetzung

Dezentrales Management von Notfallinformationen

Darüber hinaus gab es in Schleswig-Holstein bereits GDIS 2, das ein dort ansässiges Medizintechnikunternehmen als Pilotprojekt betrieb. Damit konnte auch ermittelt werden, welche Krankenhaus- und Transportkapazitäten für die konkrete Art des Notfalls zur Verfügung standen und welche Transportzeiten aufgrund der akuten Verkehrslage vom jeweiligen Flughafen anfallen würden. Auf dieser Basis schlug GDIS 2 einen Notlandeplatz vor, den der Flugkapitän akzeptierte. Daraufhin errechnete der Bordcomputer die optimale Anfluglösung, und alle verfügbaren Informationen über den Notfall und die Ankunftszeit des Flugzeuges wurden automatisch an den Flughafen, die Rettungs- und Transportdienste und das Krankenhaus übermittelt.

Kontrollierte Datenverarbeitung sensitiver Informationen bei geschlossener Informationskette

Während des Anfluges wurden die Sensordaten des Medicus verschlüsselt an einen Fernarzt übertragen, der der Stewardess weitere Anweisungen über das GDIS 2 zur Stabilisierung des Patienten erteilte. Der Medicus gab die dazu notwendigen Medikamente in richtiger Dosierung aus seinem Inneren frei.

Automatische Übertragung und Analyse medizinischer Informationen

Nach der Landung öffnete sich die Flugzeugtür und Notfallmediziner brachten den Mann in die Ambulanz. Der Notarzt entnahm dem Medicus die Notfallkarte mit allen Sensordaten, Informationen über erfolgte Maßnahmen und bisherige Datenübermittlungen an den Fernarzt.

Diese würde er in der Notfallambulanz einlesen und vom dortigen Computer weitere Diagnoseschritte sowie Behandlungs- und Medikamentierungsvorschläge für den Transport erhalten. Gleichzeitig würden die Sensordaten und die im Krankenwagen getroffenen Maßnahmen der Notfallkarte hinzugefügt, um dem behandelnden Arzt im Krankenhaus eine vollständige Dokumentation der Krankengeschichte zu liefern. Hier werden weitere Behandlungsdaten aus Sensoren, ärztlichen Diagno-

sen und gezielt verabreichte Medikamentenmengen hinzugefügt. Nach dem Ende einer stationären Behandlung würde die Karte dann dem Patienten übergeben werden, damit dieser seine Ärzte umfassend über die Vorgeschichte informieren kann – oder auch nicht. Wenn selbst die geschwindigkeitsoptimierte Behandlung nicht mehr helfen konnte erleichtert die Karte dem Gerichtsmediziner die Arbeit. … Letzteres war hier nicht notwendig gewesen.

Bewusstsein für Privatsphäre

Während wir unseren Weg ins Baltikum mit nur 60 Minuten Verspätung fortsetzten, hörte ich, wie sich zwei andere Passagiere über die Geschwindigkeit und die Reibungslosigkeit des Notfalleinsatzes wunderten, würde sich die Kofferlogistik der Flughäfen daran doch einmal ein Beispiel nehmen …, aber das ist eine andere Geschichte ubiquitären Computings.

Optimierung von Verkehrsströmen auch bei unvorhersehbaren Zwischenfällen

5 Auswirkungen der UC-Technologie auf Verbraucher: Chancen und Risiken

Sarah Spiekermann

UC hat sich in den letzten Jahren zu einem immer wichtiger werdenden Forschungsfeld entwickelt. Jedoch gibt es kaum einen technisch oder ökonomisch ausgerichteten Artikel, der neben den Chancen und Möglichkeiten der Technologie nicht auch auf die mit ihr einhergehenden sozialen Risiken zumindest hinweisen würde.

Der vorliegende Bericht hat daher zum Ziel, die Auswirkungen des UC mit seinen Chancen und Risiken für Verbraucher zu beleuchten. Bei der Erläuterung von Chancen geht es dabei hauptsächlich um die heute bekannten Einstellungen von Verbrauchern zu UC-Anwendungen. Sehen sie einen Nutzen in der Technik und worin besteht dieser? Wovon hängt der Nutzen ab? Und welche Bevölkerungsgruppen könnten von UC-Diensten am meisten profitieren? Zur Beantwortung dieser Fragen wird von einer empirischen Studie berichtet, welche in Kooperation mit der Wochenzeitung DIE ZEIT im November 2005 mit über 5.000 Teilnehmern in Deutschland durchgeführt wurde.

Neben der Darstellung von Nutzen und Vorteilen wird im zweiten Teil dieses Kapitels dann über die potenziellen Schattenseiten von UC-Technologie berichtet. Es wird darauf eingegangen, welche Rolle die informationelle und physische Selbstbestimmung für Menschen in UC-Umgebungen spielt. Und es wird anhand der Ergebnisse der Empirie untersucht, wie wichtig der Datenschutz für die deutsche Bevölkerung wirklich ist. Ferner wird aufgezeigt, wie wichtig die finale Kontrolle des Menschen über die allgegenwärtige Rechnerumgebung ist, im Sinne der Aufrechterhaltung gesellschaftlicher Normen ebenso wie zur Gewährleistung von Technikakzeptanz.

5.1 Chancen der UC-Technologie

Technischer Fortschritt ist im Weltbild der westlichen Moderne häufig positiv belegt. Bleibt man dieser kulturoptimistischen Tradition treu, so ist auch die UC-Technologie als grundsätzlich positiv und chancenreich zu beurteilen, da sie zum einen eine Fülle neuer Produktfunktionen und Services ermöglicht (und damit eine qualitative Verbesserung der Lebenssituation verspricht) und zum anderen das Potenzial hat die Produktivität gegenwärtiger Arbeitsprozesse zu steigern.

Dieser Bericht zeigt an vielen Stellen auf, wie herkömmliche Produkte durch UC-Technologie mit Zusatzfunktionalitäten ausgestattet werden können. Als Beispiel kann, wo bisher Zahnbürste und Spiegel als stumme Gebrauchsgüter dienten, durch RFID und Sensoren eine neue Funktionalität entstehen, wie etwa die spielerische Kontrolle von Kindern bei der Zahnpflege. Räume und Fahrzeuge können sich unseren Bedürfnissen automatisch anpassen. Zugangskontrollen können automatisiert und vereinfacht werden.

Ebenso können völlig neue Anwendungen entstehen. Die Fülle denkbarer neuer Services ist immens und verspricht Verbrauchern in vielen Lebensbereichen einen Nutzengewinn durch

Zeitersparnis, neue Freizeitbeschäftigungen, mehr Kommunikationsmöglichkeiten, verbesserte medizinische Frühwarnsysteme usw.

Zu erwarten ist, dass sich durch solche Services auch die sozialen Beziehungen zwischen Menschen ändern werden. Auf welche Weise kann man heute freilich nicht wissen. Welche Rolle kommt einer Mutter zu, wenn das Kind die Zahnputztechniken besser vom Spiegel lernt als von seiner Bezugsperson? Inwieweit kann virtuelle Nähe tatsächliche räumliche Nähe ersetzen? Welcher sozialen Dynamik unterliegen Beziehungen zwischen Menschen, wenn jeder jeden überwachen kann und vielleicht schon von Kindheit an an diesen Prozess gewöhnt worden ist?

Die Tatsache, dass Aktivitäten, die vorher eine Interaktion zwischen Menschen ausgelöst haben, nun durch eine Interaktion zwischen Mensch und Maschine teilweise abgelöst werden, wird zwangsläufig zu einer neuen Generation sozialer Beziehungsqualitäten führen.

Neben dieser direkten Auswirkung der UC-Technik auf das menschliche Leben wird es ökonomisch bedingte indirekte Auswirkungen geben. Insbesondere ist zu erwarten, dass das Innovationspotenzial der neuen Technologien zu wirtschaftlichem Wachstum führt. Immerhin birgt fast jedes Produkt das Potenzial einer „digitalen Aufrüstung“. Diese digitale Aufrüstung erschließt für viele Produkte Differenzierungspotenziale und erlaubt neue Produktlebenszyklen. Dies wiederum kann zu neuen Absatzmärkten führen und den Erhalt von Arbeitsplätzen positiv beeinflussen.[341] Die ökonomischen Bestimmungsfaktoren des UC, welche im vorderen Teil dieser Studie dargestellt worden sind, haben die ökonomischen Potenziale bereits in größerem Detail beschrieben. Entscheidend ist jedoch, dass die technischen Innovationsmöglichkeiten nur dann zu Wachstum führen, wenn diese von Konsumenten auch angenommen und nachgefragt werden; wenn sie also in der Lage sind, neue Absatzmärkte zu bedienen. Vor diesem Hintergrund soll das folgende Kapital über die Wahrnehmung des Nutzens von UC-Technik berichten bzw. von Produkten, die heute bereits UC-Technik enthalten. Es soll auf Basis von empirischen Befunden erste Erkenntnisse darüber liefern, was die Kaufbereitschaft und Nutzungsintention von UC-basierten Diensten fördert und welche technischen Gestaltungsformen möglicherweise zu einem Scheitern der neuen Produktfunktionalitäten führen können.

5.1.1 Wahrnehmung von Nutzen der RFID-Technik durch Verbraucher

Ubiquitous Computing, insbesondere RFID- und Sensortechnik ist heute in viele Produkte und Dienstleistungsinfrastrukturen integriert. So hat sich in Deutschland rund um die Automobilbranche eine Industrie für Sensortechnik entwickelt. In einen neuen Mercedes verbaut Daimler Chrysler beispielsweise zwischen 50 bis 150 Sensoren.[342] Gleichzeitig wächst die

[341] Sicherlich gibt es auch gegenläufige Auswirkungen der UC-Technik auf den Arbeitsmarkt, denn es ist nicht auszuschließen, dass durch Technologien wie RFID Personal ersetzt werden kann. Wie die einzelnen Effekte der Technologie auf den Arbeitsmarkt wirken, ist derzeit jedoch nicht erforscht, und es kann hier keine Aussage dazu gemacht werden.

[342] Technology Review vom 20.01.2004: Das Auto fühlt mit.

Industrie für RFID-Anwendungen jeder Art: ob im Autoschlüssel, beim Bibliotheksmanagement oder in der industriellen Fertigung.

Die meisten dieser auf UC-Technologie basierenden Produkte und Dienstleistungen scheinen von Verbrauchern positiv angenommen zu werden. Dazu gehört beispielsweise der von vielen Skifahrern begrüßte und mit RFID aufgerüstete Skipass, welcher es Wintersportlern erlaubt, Liftkontrollen „reibungsloser" zu passieren. Ebenso führen öffentliche Verkehrsbetriebe derzeit vergleichbare kontaktlose Zugangsservices ein, welche für Verbraucher zu Zeitersparnissen führen sollen und Kontrollen vereinfachen.

Fraglich ist jedoch, ob die Akzeptanz der neuen UC-Dienstleistungen ebenso positiv zu beobachten wäre, wenn Kunden wüssten, dass die elektronische Registrierung mittels RFID zur Erstellung von Bewegungsprofilen herangezogen werden kann; dass die neuen Services also Technologieeigenschaften besitzen, die in der Lage sind, die informationelle Selbstbestimmung zu unterminieren. Immer wieder kommt es vor diesem Hintergrund zu Demonstrationen vor den Geschäften solcher Unternehmen, die die Einführung von RFID planen. Ein Beispiel ist die Boycott Bennetton-Kampagne in den USA[343] oder Demonstrationen vor dem Metro Future Store in Rheinberg.[344]

Solche Vorfälle zeigen, dass die Akzeptanz von UC-Technologie, obgleich zunächst scheinbar vorhanden, letztlich umstritten ist. Unternehmen, welche sich dieses Innovationsfeld heute zunutze machen wollen und dabei negative Presse vermeiden möchten, müssen also berücksichtigen, wie die Privatsphäre von Kunden gewährleistet werden kann und welche Alternativen und Kontrollen dem Kunden geboten werden müssen, damit dieser die Technologie akzeptiert. Ebenso wichtig ist ein Verständnis dafür, welche Nutzenvorteile von Kunden im Umgang mit UC-basierten Produkten und Diensten wahrgenommen werden und als wie wichtig diese eingeschätzt werden. Studien des Auto-ID Labs[345] sowie eine in 2004 für den deutschen Einzelhandel durchgeführte Studie belegen dies eindeutig.[346]

Bei der in Deutschland mit über 200 Verbrauchern durchgeführten Studie zeigt sich, dass Kunden eine ganze Reihe von RFID-basierten Dienstleistungen in und außerhalb von Supermärkten durchaus schätzen. Dazu gehört im Laden beispielsweise die Fähigkeit von Verkaufspersonal, Lagerbestände automatisch prüfen zu können, die Gewährleistung verbesserter Herkunftskontrollen von Lebensmitteln sowie eine verbesserte Verfügbarkeit von Waren, für die man sich extra in einen Laden begeben hat (für Details siehe Abbildung 8).[347] Nach dem Kauf wird geschätzt, ohne Bon auf Garantieansprüche zurückgreifen zu können, neue Informationsdienste zu Produkten nutzen zu können und intelligente Funktionen von

[343] http://www.boycottbenetton.com/ (29.03.2006).

[344] http://www.governet.de/themen/datenschutz/28548.html (29.03.2006).

[345] Duce: Public Policy: Understanding Public Opinion. A.-I. Center, Cambridge, UK, University of Cambridge, UK, 2003.

[346] Guenther / Spiekermann: RFID and Perceived Control - The Consumer's View, Communications of the ACM 48(9), 2005, S. 73-76.

[347] Ibid.

Medikamentenschränken oder Waschmaschinen zur Verfügung zu haben. Überwiegend empfindet eine Mehrheit der Verbraucher solche Möglichkeiten als angenehm bis sehr angenehm (für Details siehe Abbildung 9). Zu dieser positiven Einschätzung kommt es trotz einer ausführlichen Information der Teilnehmer über RFID vor der Befragung mittels eines auf Neutralität geprüften Films (in welchem die Möglichkeiten von RFID und die potenziellen Gefahren für den eigenen Datenschutz ausführlich dargestellt werden).

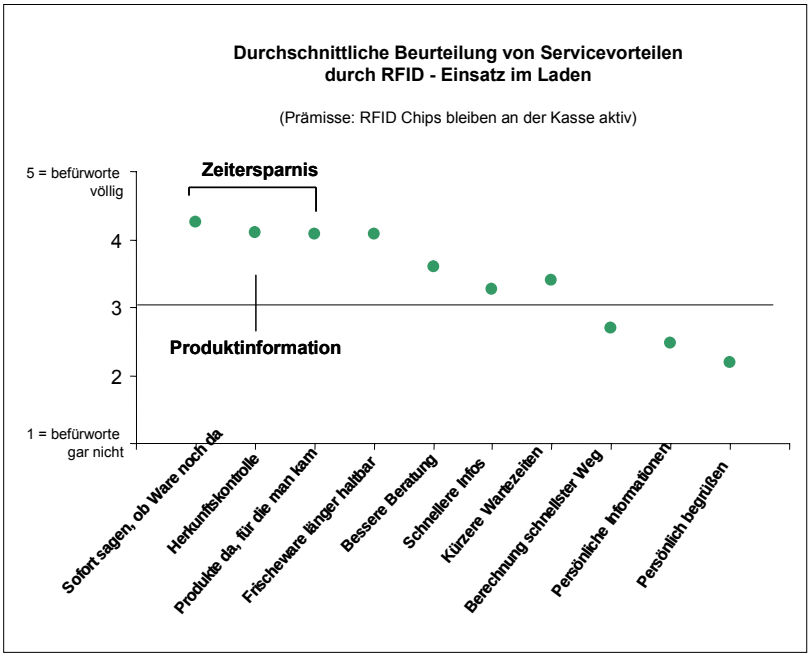


Abbildung 8: Beurteilung von Nutzenpotenzialen durch den RFID-Einsatz im Handel

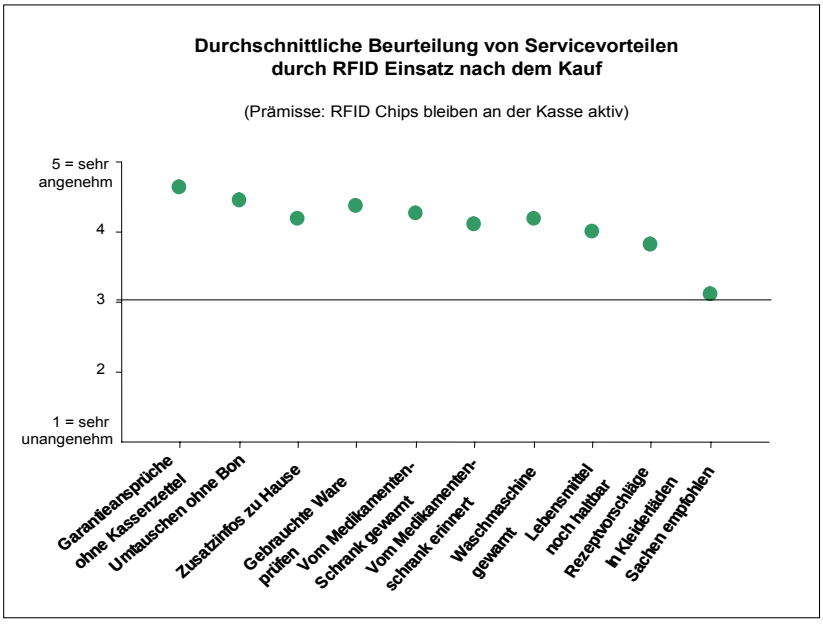


Abbildung 9: Beurteilung von Nutzenpotenzialen durch den RFID-Einsatz nach dem Kauf

Neben den hier untersuchten Informationsdiensten im Einzelhandel bietet die RFID- und Sensortechnik noch eine ganze Reihe anderer Nutzenvorteile für Verbraucher. Insbesondere

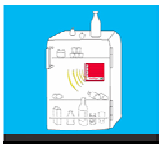
können Interaktionen zwischen Menschen und Objekten automatisiert werden. Ein Beispiel sind automatische Zugangskontrollen oder automatische Anpassungen der Umgebung auf jeden Einzelnen. Fraglich ist jedoch, wie Verbraucher diese Automatisierungen beurteilen und ob und unter welchen Bedingungen sie diese als so nützlich empfinden, dass sie daran interessiert sind, diese zu kaufen. Der folgende Abschnitt soll diese Fragestellung näher untersuchen.

5.1.2 Beurteilung von Automatisierung durch Ubiquitous Computing

Die Beurteilung der Nützlichkeit einer Technologie ist von großer Bedeutung für ihre Akzeptanz. Durch eine ganze Reihe von Studien in den USA ist in den letzten 15 Jahren das so genannte „Technologieakzeptanzmodell“ nachgewiesen worden, welches die wahrgenommene Nützlichkeit einer Technologie neben deren Einfachheit (in der Bedienung) als den wichtigsten Faktor für ihre nachhaltige Adoption postuliert.[348] Nützlichkeit und Einfachheit haben sich sogar als noch wichtiger für die Akzeptanz herauskristallisiert als etwa Einstellungen und Werte, die das Verhalten von Menschen ebenso nachgewiesen steuern können.[349]

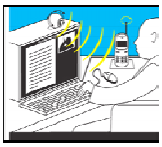
Vor dem Hintergrund dieses theoretisch fundierten Modells hat die Beurteilung der Nützlichkeit und Einfachheit von UC-Technologien auch einen Schwerpunkt einer Verbraucherstudie gebildet, welche in Kooperation mit der Wochenzeitung DIE ZEIT für den vorliegenden Bericht durchgeführt worden ist. Kernfragen waren: Als wie nützlich und einfach beurteilen Verbraucher UC-Technologien in unterschiedlichen Kontexten? Wovon hängt die Beurteilung der Nützlichkeit ab? Und in welchem Spannungsverhältnis steht die Nützlichkeit, die Akzeptanz und etwaige Bedenken gegenüber der Technologie, insbesondere Kontrolleinbußen?

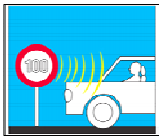
Die Nützlichkeit und Einfachheit sowie weitere Beurteilungsparameter wurden anhand von vier verschiedenen UC-Szenarien getestet, die die Studienteilnehmer ausführlich bewerten mussten (Appendix 1 enthält eine ausführliche Beschreibung der Studiendurchführung). Die Szenarien (Appendix 2 bis 5) bezogen sich auf…

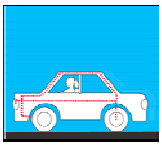
1  … einen Kühlschrank, der den eigenen Warenbestand prüft und nachbestellt, wenn etwas fehlt.

[348] Venkatesh / Davis: A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies, Management Science 46(2), 2000, S. 186-204.
Davis: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, MIS Quarterly 13(3), 1989, S. 319-340.

[349] Davis / Bagozzi et al.: User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, Management Science 35(8), 1989, S. 982-1003.

2  … einen Computerarbeitsplatz, der automatisch alle angeschlossenen Geräte, insbesondere Kamera und Telefon, an den Nutzer anpasst.

3  … ein Auto, welches automatisch abbremst, wenn der Fahrer zu schnell fährt.

4  … ein Auto, welches sich automatisch selbst wartet und für einen Werkstatttermin sorgt, wenn etwas kaputt zu gehen droht.

Die Szenarien wurden mit jeweils 2 Grafiken und einem kurzen Text beschrieben. Insgesamt nahmen über 8.000 Personen an der Befragung teil, die sowohl online als auch auf Papier im November 2005 durchgeführt wurde. 4.744 Teilnehmer füllten die Befragung bis zum Ende aus und konnten daher in die vorliegende Analyse mit einbezogen werden. Die Teilnehmer hatten die Wahl, wie viele der Zukunftsszenarien sie anschauen und bewerten wollten. 75% entschlossen sich, alle vier Szenarien zu bewerten, 20% wählten zwei Szenarien und 5% drei Szenarien.

Da die Befragung in Kooperation mit der Wochenzeitung DIE ZEIT durchgeführt und auch im Heise-Newsticker darüber berichtet wurde, unterlag sie nicht nur einer starken Selbstselektion (die viele Befragungen mit sich bringen), sondern sie spiegelt vor allem die Einschätzung besser gebildeter (90 % der Befragten haben mindestens Abitur), jüngerer (70 % sind unter 40 Jahre) und online affiner (68% erledigen ihre Arbeit fast ausschließlich oder ausschließlich am Computer) deutscher Männer (80% männlich) wieder. 200 weitere Personen wurden deshalb darüber hinaus auf Papier befragt. Hier erfolgte die Auswahl der Teilnehmer mit Hilfe einer Marktforschungsagentur. Es wurde eine Stichprobe befragt, die der soziodemographischen Struktur der deutschen Bevölkerung nahe kommt, wenn auch hier mit einem leicht erhöhten Bildungsanteil (51 % weiblich, 49 % männlich; 45 % unter 40 Jahre; 43 % mit Abitur; 38 % erledigen Arbeit am Rechner).[350] Wenn im Folgenden über die Ergebnisse berichtet wird, ist der Papierstudie vor diesem Hintergrund eine größere Aussagefähigkeit über das Denken der deutschen Bevölkerung zuzusprechen als der online erhobenen Stichprobe. Appendix 6 gibt einen genauen Überblick über die soziodemographische Struktur der Stu-

[350] Die Befragung durch die Agentur ist statistisch gesehen nicht repräsentativ für die deutsche Bevölkerung, da keine Zufallsstichprobe in Gesamtdeutschland gezogen wurde. Vielmehr wurde bei der begrenzten Zahl von 200 Befragungsteilnehmern darauf geachtet, dass die soziodemographische Zusammensetzung der Stichprobe nach Alter, Geschlecht, Bildung und Einkommen in etwa die Verhältnisse wiederspiegelt, welche in Deutschland heute vorherrschen. Hier sind laut dem statistischen Bundesamt 49% männlich und 51% weiblich, 55% sind unter 45 Jahre alt und 22% haben eine Hochschulreife erreicht.

dienteilnehmer beider Stichproben.

Bei der Betrachtung der Antworten auf Fragen zur Nützlichkeit der Technologie sowie zur emotionalen Bewertung der Szenarien zeigen die Mittelwerte, dass die Befragten den neuen Technologien insgesamt passiv und unentschlossen gegenüberstehen, jedoch mit einer eher positiven als negativen Tendenz (siehe Appendix 8 für Details). Insbesondere die Selbstwartungsfunktion von Autos führt zu einer durchweg positiven Bewertung. Dieses ist das am positivsten bewertete UC-Szenario. Eine Bremsautomatik im Auto hingegen wird als eher unnütz empfunden. Und ein sich automatisch anpassender Arbeitsplatz löst eher negative emotionale Reaktionen hervor. Beim Vergleich der beiden Stichproben zeigt sich, dass die Bewertung durch die auf Papier befragten Personen durchweg besser ist. Sie nehmen die präsentierten UC-Services als relativ nützlicher und emotional ansprechender wahr. Dieser Unterschied ist fast durchgängig statistisch signifikant.[351]

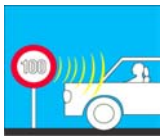
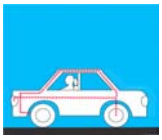
				
Emotionale Reaktion (heiter? trübsinnig? froh?)	**passiv – positiv** 👍	**passiv – negativ** 👎	**passiv – positiv** 👍	**positiv** 👍👍
Beurteilung der Nützlichkeit	**unentschlossen – eher nützlich** 👍	**unentschlossen – eher nützlich** 👍	**unentschlossen – eher weniger nützlich** 👎	**nützlich** 👍👍
Beurteilung der Einfachheit	**einfach** 👍👍	**unentschlossen – eher einfach** 👍	**einfach** 👍👍	**einfach** 👍👍

Tabelle 5: Durchschnittliche Beurteilung des beschriebenen Service

Interessant ist, dass die Beurteilung der Einfachheit aller präsentierten UC-Anwendungen fast durchweg positiv ist. Die Teilnehmer erwarten kaum Bedienungsschwierigkeiten. Dies ist konform mit dem Grundgedanken des Ubiquitous Computing, demzufolge die Technik ja auch „calm“ (zu Deutsch „ruhig“) sein soll, dem Benutzer also relativ wenig bis gar kein Können mehr abverlangt.[352] Bei der Beurteilung der Einfachheit gab es keine signifikanten Unterschiede zwischen der Onlinestichprobe und den auf Papier Befragten.

Laut dem oben erläuterten Technologieakzeptanzmodell ist die Beurteilung von Nützlichkeit

[351] „Statistisch signifikant“ heißt hier, dass ein gemessener Unterschied zwischen zwei Gruppen mit einer Wahrscheinlichkeit von 95% nicht zufällig gemessen wurde. Wenn im Folgenden das Wort „signifikant“ im Text gebraucht wird, dann handelt es sich immer um eine statistische Signifikanz in diesem Sinne.

[352] Weiser / Brown: The Coming Age of Calm Technology, Xerox Parc, 1996.

und Einfachheit ein guter Indikator für die Nutzerakzeptanz. Nutzerakzeptanz wurde in der vorliegenden Studie als Kauf- und Nutzungsintention gemessen. Erwartungsgemäß zeigen die Teilnehmer auch hier Unentschlossenheit (siehe Appendix 8). Die *Nutzungs*intention hat dabei eine eher positive Tendenz, die *Kauf*intention eine eher negative. Kauf- und Nutzungsintention sind für die Fahrzeugfunktionen bei der Papierbefragung signifikant höher als bei der Onlinebefragung (wobei die Kaufintention nur für die Heimanwendungen gemessen wurde).

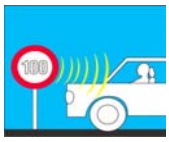
				
Nutzungs-intention	**unentschlossen - positiv** 👍	**unentschlossen-positiv** 👍	**unentschlossen-positiv** 👍	**unentschlossen-positiv** 👍
Kaufintention	**unentschlossen – eher negativ** 👎	**unentschlossen – eher negativ** 👎	**k.a.**	**k.a.**

Tabelle 6: Durchschnittliche Intention zu nutzen und zu kaufen

Entscheidend ist selbstverständlich, dass der Erkenntnisgewinn zur UC-Akzeptanz sich nicht auf die absolute Bewertung dieser limitierten Anzahl von vier Szenarien beschränkt. Vielmehr ist entscheidend, dass durch die Befragung in einem nächsten Schritt generalisierbare Aussagen abgeleitet werden können, wie bedeutsam Nützlichkeit, Emotionen und Einfachheit der Bedienung für Kauf und Nutzung von UC-Services insgesamt sind. Ebenso ist wichtig zu verstehen, wovon diese abhängen. Zu diesem Zweck wurde ein Hypothesenmodell aufgestellt. Es postuliert, dass die Nützlichkeit von UC-Services davon abhängt, wie kompetent man sich in dem jeweiligen Anwendungsgebiet sieht, welches automatisiert werden soll (domänenspezifische Kompetenz) und wie viel Spaß man an diesem hat (intrinsische Motivation). Fühlt man sich kompetent in und hat man Spaß an einer Sache, wie etwa einzukaufen, so wird man eine Automatisierung dieser Tätigkeit wahrscheinlich als weniger nützlich ansehen. Vertrauen in ein System und Kontrolle über dasselbige sind Faktoren, von denen wir einen hohen Einfluss auf die affektive Bewertung erwartet haben. Fehlen Vertrauen und Kontrolle, so wird die emotionale Reaktion auf ein System negativ ausfallen. Technologische Kompetenz ist mehrfach als ein Indikator für die wahrgenommene Einfachheit eines Systems postuliert worden, denn wer sich mehr zutraut im Umgang mit technischen Geräten, wird möglicherweise auch bei UC-Services keine Nutzungsschwierigkeiten absehen. Und unterschiedliche Risikofacetten sind schließlich in der Konsumentenforschung schon lange als

wichtige Kauf- und Nutzungsindikatoren erkannt worden[353], deren individuelle Einflüsse möglicherweise auch auf die Akzeptanz von Produkten und Diensten wirken können. All diese Faktoren, welche Wechselwirkungen aufzeigen und letztendlich in die Intention münden, einen UC-Service zu nutzen und/oder zu kaufen, wurden entweder aus der Literatur abgeleitet[354] oder stellten sich im Rahmen von fünf vorbereitenden Interviews und einer Fokusgruppe als relevant heraus (siehe dazu auch Annex 7 mit Beschreibung der Studiendurchführung).

Auf Basis der gesammelten Daten konnte dann für alle Szenarien ein statistisch valides Modell entwickelt werden.[355] Das Modell wurde separat für die Papier- und die Onlinestichprobe geprüft, und es zeigte sich, dass für beide Stichproben eine ähnliche Modellstruktur nachzuweisen ist. Abbildung 4 stellt das Modell für die Papierstudie grafisch dar. Die Zahlen zwischen den Konstrukten sind Kennzahlen, welche für die Stärke des Einflusses stehen, den ein Konstrukt auf das andere ausübt.[356]

[353] Cox: Synthesis: Risk taking and information handling in consumer behavior. Boston, MA, Harvard University Press,1967, S. 604-639, Cunningham: The Major Dimensions of Perceived Risk, Risk Taking and Information Handling in Consumer Behavior. D. Cox. Cambridge, MA, Harvard University Press, 1967.

[354] Als theoretische Grundlage dienten hier theoretische Arbeiten zur Technologieakzeptanz, Theory of Reasoned Action, Theory of Planned Behavior, zur Kontrollwahrnehmung, zur Rolle von wahrgenommenem Risiko sowie zur Umweltpsychologie.

[355] Konkret wurde für den vorliegenden Bericht eine Reihe von multiplen Regressionsanalysen gerechnet. Weitere statistische Analysen, wie etwa Strukturgleichungsmodelle, wurden ebenfalls durchgeführt. Über diese Modelle, die in ihren Kernaussagen weitestgehend identisch sind, wird an anderer Stelle berichtet werden.

[356] Die Zahlen entsprechen dem Durchschnitt aller ß-Gewichte*100, der sich über die vier Szenarien hinweg ergibt. Die ß-Gewichte, welche ein Maß sind für den Einfluss einer unabhängigen Variablen auf eine abhängige Variable, wurden jeweils im Rahmen der Regressionsanalysen ermittelt. In der Grafik sind nur solche Einflüsse abgetragen, welche sich für alle Szenarien hinweg als jeweils statistisch signifikant herausgestellt haben. In Appendix 7 befindet sich eine genaue Übersicht über alle Beta-Gewichte*100, die sich pro Szenario pro Regressionsgleichung ergeben.

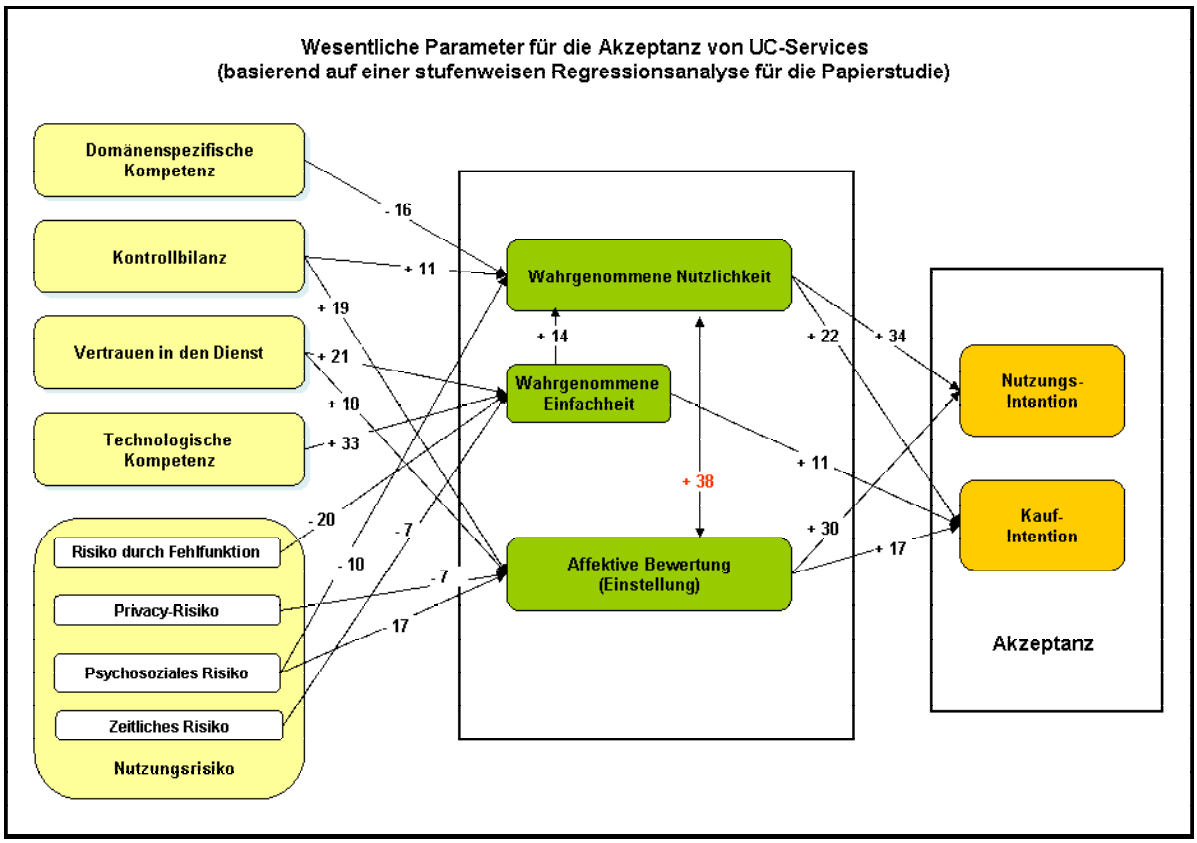


Abbildung 10: Abhängigkeiten in der Beurteilung der UC-Szenarien

Hier zeigt sich, dass die wahrgenommene Nützlichkeit eines Service – ähnlich wie in früheren Untersuchungen im PC-Umfeld – der wichtigste Indikator für die Nutzungs- und auch die Kaufintention ist. Interessanterweise sind es jedoch weniger praktische Erwägungen, die die Einschätzung von Nützlichkeit eines UC-Service beeinflussen. Vielmehr wird Nützlichkeit über alle Szenarien hinweg zum größten Teil durch die affektive Bewertung eines Szenarios erklärt. Affektive Bewertung ist ein Maß für die Zufriedenheit bzw. Unzufriedenheit, die ein Szenario bei seinen Betrachtern auslöst. Diese affektive Bewertung wiederum ist laut unserer Datenbasis am stärksten abhängig von dem Grad der Kontrolle, den ein Teilnehmer über die Technologie empfindet. Auch der Grad des Vertrauens in den Dienst und die Wahrnehmung, dass der Dienst in den eigenen Alltag passt (psychosoziales Risiko) spielen eine wichtige Rolle. Die intrinsische Motivation bzw. der Spaß an einer Tätigkeit, die mit UC-Technik automatisiert werden soll, hingegen hat sich als unwichtig herausgestellt. Für die Praxis bedeutet dies, dass Anbieter von UC-Services und Produkten großen Wert darauf legen sollten, dem Kunden maximale Kontrolle im Umgang mit der Technik zu geben.

Ein weiterer Faktor, welcher für die Nützlichkeit und damit für die Akzeptanz eine Rolle spielt, ist die domänenspezifische Kompetenz, die jemand in dem Bereich empfindet, wo Automation entstehen soll. Daher: Wenn jemand meint, dass er ohne die Automation besser zurecht kommt, dann nimmt die Nützlichkeit ab. Jemand, der die Einstellungen an seinem Arbeitsplatz optimal „in Schuss“ hat, findet die Automatisierung von Einstellungen unnütz. Jemand, dem selten etwas im Kühlschrank fehlt, braucht keine intelligente Funktion zu dessen Auffüllung. Für die Praxis bedeutet dies, dass bei der Vermarktung von UC-Services und Produk-

ten Wert darauf gelegt werden sollte, wem man diese anbietet. Es ist denkbar, dass in vielen Fällen intelligente Funktionen vor allem Nischenmärkte ansprechen. Eine Vermarktung von UC-Produkten „nach dem Gießkannenprinzip“ wird daher wahrscheinlich häufig keinen Sinn machen. Eine weitere Analyse, die diese Erkenntnis stützt ist eine zweifaktorielle Varianzanalyse, mit der Unterschiede zwischen Personen mit verschiedenen soziodemografischen Eigenschaften hinsichtlich ihrer Bewertungen der Technologien analysiert wurden (Alter, Geschlecht, Bildung etc.). Hier zeigt sich, dass Leute in unterschiedlichen Altersklassen UC-Services unterschiedlich bewerten: Insbesondere nehmen junge Leute (bis 29 Jahre) und Senioren (über 60 Jahre) die beschriebenen Dienste als besonders nützlich wahr (siehe Abbildung 11). Eine Erklärung dafür könnte sein, dass älteren Leuten die Umsicht im Straßenverkehr schwer fällt, ebenso wie das Einkaufen, und dass sie hier eine Entlastung durch UC-Technologien begrüßen würden. Junge Leute hingegen reizt möglicherweise die technische Innovation selbst. Obgleich diese Begründung nur Spekulation ist, bleibt für Anbieter von UC-Services zu bemerken, dass alle beschriebenen UC-Szenarien in gleicher Weise einen Alterstrend aufweisen, der für unterschiedliche Vermarktungssegmente steht.

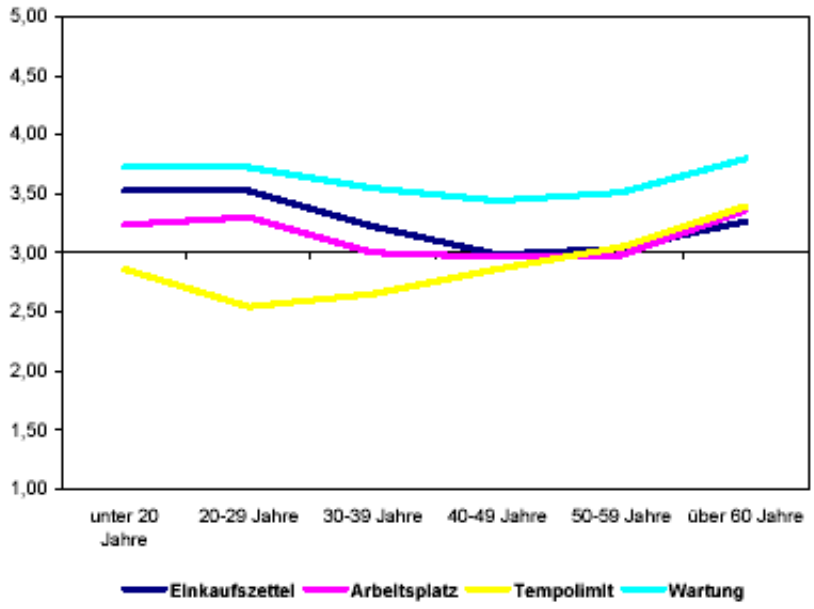


Abbildung 11: Altersunterschiede in der Nützlichkeitsbewertung je Szenario[357]

Zusammenfassend lässt sich sagen, dass UC-Services und -Funktionen von Verbrauchern nicht abgelehnt, sondern im Gegenteil an vielen Stellen als durchaus nützlich und eher positiv beurteilt werden. Die Beurteilung der Nützlichkeit hängt zu einem großen Teil direkt und indirekt vom Grad der Kontrolle ab, die man einem Empfänger über die Technik lässt. Dieser Aspekt wird in Kap. 5.4 unten noch einmal näher erläutert. Ferner spielt das Vertrauen in das System und dessen Betreiber eine Rolle sowie eine Minimierung der Zeitinvestition auf Seiten des Nutzers. Werden diese Faktoren beachtet, so könnte sich auf Basis von UC-Technologie eine Vielfalt neuer Produkte und Dienstleistungen entwickeln, die von Verbrau-

[357] Für nähere Angaben zu den Signifikanzen der Statistik siehe Annex.

chern geschätzt werden und das wirtschaftliche Wachstum unterstützen.

5.2 Risiken der UC-Technologie

Neben diesen positiven Effekten gibt es auch eine Reihe von potenziell negativen Auswirkungen der UC-Technik. Auf diese soll im Folgenden näher eingegangen werden.

Viele Schriften ordnen negative soziale Auswirkungen des UC unter dem recht pauschalen Schlagwort Privacy (zu Deutsch „Privatsphäre“) ein.[358] Sie argumentieren, dass durch allgegenwärtige Rechnerumgebungen die Privatsphäre von Menschen in ihren unterschiedlichen Rollen – als Privatperson wie auch als Arbeitnehmer – bedroht sei. Dabei bleibt zumeist unklar, um welche Art von Privatsphäre es sich handelt, die hier bedroht scheint. Ist es der Schutz der eigenen personenbezogenen Informationen (zu Englisch „Information Privacy“), welcher unterminiert wird? Oder sogar die physisch leibliche Privatsphäre, die durch unsichtbare RFID-Lesevorgänge bedroht sein könnte? Geht es um die Intimitäten und Geheimnisse einzelner Menschen, die hier bewahrt werden möchten? Oder vielmehr um ein Recht auf informationelle Selbstbestimmung als Grundlage für eine freie und demokratische Kommunikationsverfassung, so wie es im Rahmen des Volkszählungsurteils vom Bundesverfassungsgericht anerkannt wurde?[359] Die Diskussion der sozialen Bestimmungsfaktoren des UC (s.o.) haben bereits verdeutlicht, dass das UC die technischen Möglichkeiten birgt, Privatsphäre auf vielerlei Art und Weisen zu beeinträchtigen.[360] Entscheidend ist, die verschiedenen Dimensionen des Begriffs Privacy oder Privatsphäre zu differenzieren, wenn man sinnvolle Empfehlungen für die menschenwürdige Gestaltung des UC anstrebt und eine sparsame und sinnvolle Regulierung des UC wünscht. Ebenso entscheidend ist, die sozialen Implikationen des UC nicht auf Folgen für die Privatsphäre oder sogar nur den Datenschutz zu reduzieren. Nicht auszuschließen ist, dass die Auswirkungen von UC-Technologie für Umweltschutz und Gesundheit[361] sowie die Situation an den Arbeitsmärkten ebenso einschneidend für das menschliche Leben sein werden. Leider würde eine ausführliche Analyse dieser Themen den Umfang des vorliegenden Berichts sprengen. Wir wollen uns daher im Folgenden auf Fragen der Selbstbestimmung fokussieren, und zwar der informationellen wie auch physischen Selbstbestimmung in allgegenwärtigen Rechnerumgebungen. Ferner sollen die sozialen Herausforderungen des UC strukturiert und anhand dieser Struktur diskutiert

---

[358] Lahlou / Langheinrich: Privacy and trust issues with invisible computers, Communications of the ACM 48(3), 2005, S. 59-60. Adams / Sasse: Taming the Wolf in Sheep's Clothing: Privacy in Multimedia Communications. Multimedia99, Orlando, Florida, USA, 1999, Boyle: A Shared Vocabulary for Privacy, Fifth International Conference on Ubiquitous Computing, Seattle, Washington, 2003, Myles / Friday et al.: Preserving Privacy in Environments with Location-Based Applications. IEEE Pervasive Computing, 2, 2003, S. 56 - 64, Roussos / Moussouri: Consumer perceptions of privacy, security and trust in ubiquitous commerce, Personal and Ubiquitous Computing 8, 2004, S. 416-429.

[359] Bundesverfassungsgericht, Entscheidungssammlung, Band 65, 1 (Volkszählungsurteil).

[360] Spiekermann / Rothensee: Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing. I. f. Wirtschaftsinformatik, Berlin, Humboldt-Universität zu Berlin, 2005.

[361] Hilty: Electronic waste - an emerging risk?, Environmental Impact Assessment Review 25, 2005, S. 431– 435.

werden. Zunächst soll zu diesem Zweck grundsätzlich unterschieden werden zwischen dem regulären und dem irregulären Betrieb von UC-Systemen.

Zum irregulären Betrieb von Systemen kommt es wenn die Sicherheit eines UC-Systems kompromittiert wird. Trotz Testphasen kann nie ausgeschlossen werden, dass Systeme Schwachstellen haben. In einer allgegenwärtigen Rechnerumgebung multipliziert sich die Anzahl dieser Schwachstellen und damit der Angriffsziele. Dies ist insofern von Bedeutung, als dass es die alltäglichen Objekte sind, die angegriffen werden und nicht ein PC, den man im Notfall einfach abschalten kann. Die Implikationen eines durch Sicherheitsmängel hervorgerufenen irregulären Betriebs könnten daher einen höheren Schaden anrichten als dies in herkömmlichen Rechnerumgebungen der Fall ist. Es sollte daher darüber nachgedacht werden, welche Absicherungs- bzw. Versicherungssysteme gebraucht werden, damit Menschen nicht Opfer von Systemschwachstellen werden. Möglicherweise ist über den Ausbau von Rückversicherungssystemen nachzudenken, die es heute auch schon für solche Fälle gibt, in denen Produkte ihren Besitzern Schaden zufügen. Gerade bei Sicherheitslücken kann es darüber hinaus zu einem schwer nachweisbaren Datenmissbrauch kommen. Die gegenwärtig verschärfte Debatte um Identitätsmissbrauch im Internet zeigt dies deutlich. Entscheidend ist, dass Menschen für Fälle des Identitätsmissbrauchs Anlaufstellen haben, durch die sie schnell und reibungslos ihre (offizielle) Identität wiederherstellen können.[362]

Auch im regulären Betrieb kann es jedoch zu Fehlfunktionen kommen. Dies ist dann der Fall, wenn Softwareprogramme Fehler haben, bestimmte Aktionen nicht mehr erlauben oder einfach die Umwelt falsch interpretieren (technisch nicht einwandfrei funktionierende Systeme). Hinzu kommt, dass sich auch funktionierende Systeme, die sich im regulären Betrieb befinden, für den Nutzer so darstellen können, dass dieser meint, dass System funktioniere nicht. Oder sie können dem Nutzer Zugang zu wichtigen Funktionen verweigern (Nutzerwahrnehmung einer eingeschränkten Systemfunktionalität). Schließlich kann es zu negativen Auswirkungen durch UC-Services kommen, die sowohl regulär arbeiten, tadellos funktionieren und sich auch dem Nutzer unmittelbar positiv darstellen, die jedoch langfristige schädliche Implikationen haben (negative soziale Folgen). Die folgenden Abschnitte werden auf all diese Aspekte näher eingehen. Abbildung 12 verdeutlicht den strukturellen Aufbau der Analyse. Wir empfinden diesen insofern als wichtig, da viele „Dark Scenarios“ des Ubiquitous Computing[363] diese verschiedenen Betrachtungsebenen regelmäßig vermischen.

[362] Heute bedarf es für einen solchen Prozess im Schnitt immer noch 2 Jahre (Quelle: Solove: A Taxonomy of Privacy, University of Pennsylvania Law Review 154, 2005.)

[363] Alahuhta / De Hert et al.: Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities, Safeguards in a World of Ambient Intelligence (SWAMI), Punie, Delaitre, Maghiros and Wright. Brussels, 2005.

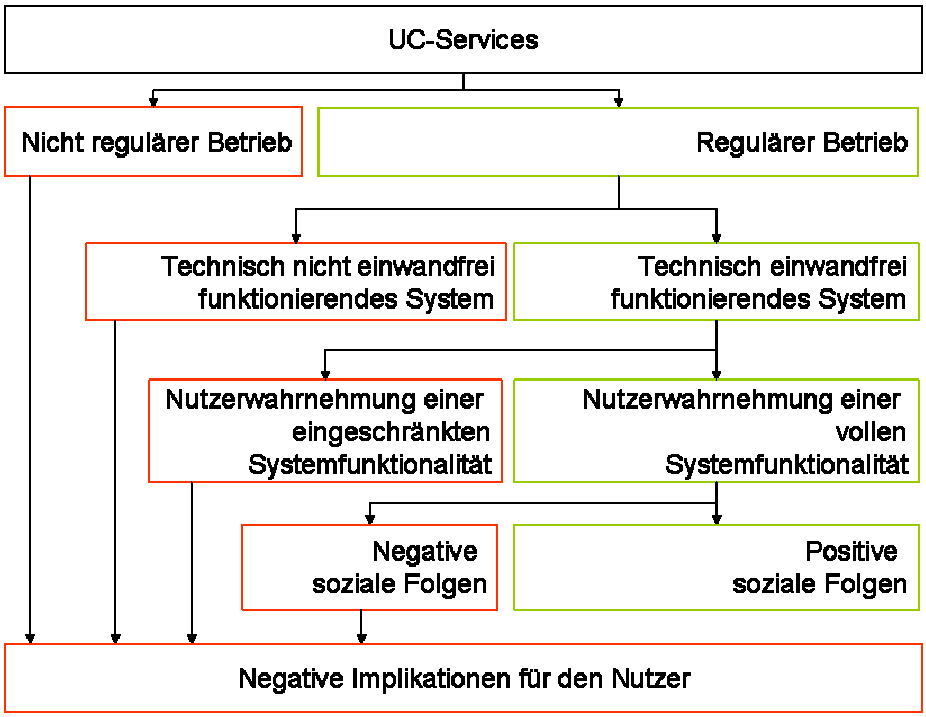


Abbildung 12: Betrachtungsebenen bei der Diskussion potenziell negativer Auswirkungen von UC-Systemen

5.2.1 Technisch nicht einwandfrei funktionierende Systeme

Nicht einwandfrei funktionierende Systeme können dadurch entstehen, dass beim Bau der Technik Fehler gemacht werden, es zu Fehlinterpretationen kommt, zu einer reduzierten Erfassung des Kontextes oder einer eingeschränkten Antizipation von Nutzerverhalten.

Technische Fehler sind heute in der Softwareentwicklung ein gängiges Problem, welches sich in der regelmäßigen Veröffentlichung von Beta-Programmversionen wiederspiegelt. Sollen Menschen jedoch mit intelligenten Objekten und sogar Umgebungen (z.B. intelligente Einkaufspassagen, Verkehrsleitsysteme etc.) interagieren und sich auf diese verlassen, darf sich eine solche „Beta-Mentalität“ der heutigen Softwareentwicklung im UC-Umfeld nicht fortpflanzen. Stattdessen sollten extensive Testphasen und Qualitätsstandards in allen Produktbereichen Vorschrift sein, um Schäden zu minimieren.

Ferner ist zu berücksichtigen, dass Technik ihre Grenzen hat; Algorithmen eben doch nicht immer die richtige Entscheidungsgrundlage liefern oder die Entscheidungsvorlagen von Menschen falsch interpretiert werden. Selbst in ausgefeilten Systemen, wie etwa im Flugzeugcockpit, ist dies häufig genug nachgewiesen worden.[364] Die Komplexität der möglichen Umweltparameter ist so groß, dass Systeme Kontexte bzw. Umweltzustände falsch interpretieren können. Es kommt zu Fehlalarm oder sogar Fehlsteuerung. Die negativen Folgen, die sich dadurch ergeben können, sind mannigfaltig. Ein Komplikationsbereich ist sicherlich der menschliche Umgang mit Alarmsystemen. Einige wissenschaftliche Arbeiten setzen sich

[364] http://techreports.larc.nasa.gov/ltrs/PDF/2004/mtg/NASA-2004-22issc-cmh.pdf (29.03.2006).

damit auseinander, welche Fehlertoleranzen in Systemen erlaubt sein sollten, bevor ein System Alarmsignale ausendet.[365] Sind diese zu groß, kommt es zu häufigen Fehlalarmsituationen mit der Gefahr, dass Menschen den Alarm in wirklich wichtigen Situationen ignorieren. Sind Fehlertoleranzen zu klein, dann besteht die Gefahr, dass eine tatsächlich wichtige, vielleicht sogar gefährliche Situation vom System nicht erkannt wird und das System versagt.

5.2.2 Wahrnehmung einer eingeschränkten Funktionalität durch den Nutzer

Selbst wenn UC-Services und –Produkte einwandfrei funktionieren, so kann es aus der Perspektive des Nutzers trotzdem zu einem nicht funktionierenden System kommen. Dies ist insbesondere dann der Fall, wenn Menschen sich durch die Bedienungskomplexität überfordert fühlen, wenn sie sich aus finanziellen Gründen entscheiden, müssen auf Funktionalität zu verzichten, die eigentlich wichtig wäre, oder wenn sie schlichtweg vergessen, ihr System zu warten. Schon heute zeigen sich diese Probleme in Ansätzen: Sehr viele und insbesondere ältere Leute nutzen Technologie seltener.[366] Die Nutzung wird erschwert, wenn sie diese auch noch warten müssen, wie etwa mit Security-Updates, neuen Programmversionen etc. Vielen Menschen fehlt schlichtweg die finanzielle Grundlage, um sich technologische Neuerungen leisten zu können, geschweige denn Hilfe bei deren Nutzung und Wartung. Es ist daher nicht auszuschließen, dass der „Digital Divide“, der sich heute auch schon innerhalb Deutschlands in Ansätzen zeigt[367], durch die Einführung allgegenwärtiger Rechnerumgebungen ausgeweitet werden könnte.

5.2.3 Potenziell negative soziale Folgen funktionierender Systeme

Zu negativen sozialen Auswirkungen von UC-Technologie kann es auch dann kommen, wenn diese aus Nutzersicht einwandfrei funktioniert, bedienbar und finanzierbar ist. Dies ist dann der Fall, wenn sich Menschen zu stark auf das Funktionieren von und den allgegenwärtigen Zugang zu Systemen verlassen, wodurch es zu ungewünschten Systemabhängigkeiten (zu Englisch „Dependence“) kommen kann. Diese können in einigen Fällen die eigene Reaktions- und Handlungsfähigkeit beeinträchtigen.[368] Ferner ist wichtig zu konstatieren, dass durch das Vorhandensein der Technik ökonomische, soziale und politische Anreize entstehen, diese so zu nutzen, dass das Individuum an vielen Stellen die Kontrolle über sei-

[365] Parasuraman / Riley: Humans and Automation: Use, Misuse, Disuse, Abuse, Human Factors and Ergonomics Society 39(2), 1997, S. 230-253.

[366] "Deutsche bei Internetnutzung im europäischen Mittelfeld": http://www.destatis.de/presse/deutsch/pm2004/p3260024.htm (29.03.2006).

[367] Groebel / Koenen et al.: Deutschland und die digitale Welt, Internet 2002: Deutschland und die digitale Welt. Internetnutzung und Medieneinschätzung in Deutschland und Nordrhein-Westfalen im internationalen Vergleich. Groebel / Gehrke; Opladen, Schriftenreihe Medienforschung der LfM,. 46, 2002.

[368] Walker / Stanton et al.: Where is Computing in Driving Cars?, International Journal of Human-Computer Interaction 13(2), 2001, S. 203-229.

ne Umgebung einbüßt ebenso wie seine informationelle Selbstbestimmung. Dadurch könnte es zu einer Reduzierung heute noch vorhandener Freiheiten kommen. Schließlich ist nicht auszuschließen, dass es durch die Erhöhung von Überwachungsmöglichkeiten der UC-Technologie zu einer für das Individuum nachteiligen Machtverschiebung gegenüber Institutionen oder anderen Individuen kommen könnte. Auch auf diesen Aspekt soll im Folgenden näher eingegangen werden.

Es sei darauf hingewiesen, dass sich die von uns hier herausgearbeiteten potenziell negativen Auswirkungen des Ubiquitous Computing in ähnlicher Form in den Arbeiten der SWAMI-Gruppe wiederspiegeln. SWAMI steht für „Safeguards in a World of Ambient Intelligence" und es handelt sich um ein Forschungsprojekt des 6. Europäischen Rahmenprogramms, welches sich ausschließlich mit den Gefahren des Ubiquitous Computing auseinandersetzt. Tabelle 7 gibt einen Überblick über die sozialen Auswirkungen, welche aus Sicht der SWAMI-Experten die wichtigsten sind.[369]

Bedeutungs-rang	Top 10 Problemkreise	Durchschnittliche geschätzte Auswirkung	Durchschnittliche geschätzte Wahrscheinlichkeit	Auswirkung x Wahrscheinlichkeit
1	Verlust von Kontrolle	4.53	4.26	19.30
2	Zunehmende Möglichkeiten der Überwachung	4.16	4.21	17.51
3	Profilbildung	3.79	4.42	16.75
4	Risiko – Vertrauen - Kriminalitätsgelegenheiten	3.47	4.16	14.44
5	Komplexität (Wert)	3.47	4.05	14.08
6	Transparentes Individuum, undurchsichtige Macht	3.89	3.53	13.73
7	Abhängigkeit	3.37	3.63	12.23
8	Nicht-partizipaktive Prozesse	3.32	3.37	11.17
9	Ausschluss	3.32	3.26	10.82
10	Kosten	2.84	3.63	10.32

Tabelle 7: Ranking der 10 wichtigsten negativen sozialen Auswirkungen des Ubiquitous Computing aus Sicht der SWAMI-Gruppe (eigene Übersetzung)

5.2.4 Remote Access versus Embodied Virtuality

Wie die Ausführungen in diesem Bericht zeigen ist die Fülle der UC-Dienste so groß, dass die Frage nahe liegt, ob man diese alle nach einheitlichen Maßstäben beurteilen und analysieren kann. Möglicherweise ist es sinnvoll, eine Struktur für die verschiedenen Anwendungstypen zu entwickeln, die eine systematische Analyse von Auswirkungen erlaubt. Eine

[369] Siehe Seite 11 in Alahuhta / De Hert et al.: Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities, Safeguards in a World of Ambient Intelligence (SWAMI), Punie / Delaitre / Maghiros / Wright, Brussels, 2005.

denkbare Möglichkeit ist auf einer hohen Ebene die Unterscheidung von zwei Diensttypen, die wir im Folgenden als „Remote Access“ (RA) sowie „Embodied Virtuality“ (EV) bezeichnen wollen.

Abbildung 13: Echtzeitbeobachtung eines Kindes durch einen Videokommunikationsrahmen[370]

Remote Access (zu Deutsch „Fernzugang“) soll im Folgenden repräsentativ für all solche UC-Services stehen, bei denen es im Kern um die Möglichkeit geht, auf entfernte Objekte, Infrastrukturen oder Personen in Echtzeit zuzugreifen, diese zu sehen und ihre Zustände zu überprüfen. Ein Beispiel für einen Remote Access-Dienst wäre etwa der in Abbildung 13 gezeigte Videokommunikationsrahmen, welcher es erlaubt, andere Menschen in Echtzeit zu sehen, mit ihnen zu sprechen, ihren Zustand festzustellen oder, im negativen Fall, sie zu überwachen.[371]

Embodied Virtuality (zu Deutsch „Verkörperte Virtualität“), welche umgekehrt auch häufig als „Augmented Reality“ bezeichnet wird (zu Deutsch „Erweiterte Realität“), bedeutet, dass unsere normale physische Umgebung durch Technologie die Möglichkeit bekommt, auf menschliches Verhalten zu reagieren bzw. mit Menschen zu interagieren. Vor dem Hintergrund dieser Interaktionsfähigkeit spricht man auch häufig von „intelligenten“ Objekten. Kang und Cuff beschreiben Embodied Virtuality wie folgt: *“[Verkörperte Virtualität … steht für eine Erweiterung von verfügbarem Wissen dahingehend, dass der materiellen Umgebung die Fähigkeit zur intelligenten Aktion und Reaktion eingehaucht wird, zur Datensammlung, Überwachung und vernetzten Information.]“*[372]

Selbstverständlich ist es möglich, dass ein intelligentes Objekt auch eine Mischung aus beiden Anwendungstypen sein kann. Zum Beispiel könnte ein interaktiver Spiegel zugleich als Kommunikationsschnittstelle dienen. Je nachdem welche Funktion aber im Vordergrund

---

[370] http://www.soft.uni-linz.ac.at/ (01.11.2005).

[371] Prototyp vorgestellt vom Institut für Pervasive Computing der Universität Linz: http://www.soft.uni-linz.ac.at/ (29.03.2006).

[372] Kang / Cuff: Pervasive Computing: Embedding the Public Sphere, Public Law & Legal Theory Research Paper Series, Los Angeles, US, University of California, Los Angeles School of Law, 2005, S. 62. :*[Embodied Virtuality]… is knowledge extended such that the material environment is infused also with intelligent action and reaction, data gathering, surveillance, and networked information*.“

steht, sind Kontrollverluste unterschiedlicher Natur und Überwachungsaspekte (zu Englisch „Surveillance“) spielen eine unterschiedlich starke Rolle. Die folgenden Abschnitte sollen darlegen, welche ökonomischen, sozialen und politischen Motive negative soziale Entwicklungen bei RA- und EV-Anwendungen fördern können, welche offenen Fragen bestehen und wo es zu Überwachungs- und Kontrollproblemen kommen könnte.

5.3 Risiken von „Remote Access“ und deren Wahrnehmung

Remote Access-Anwendungen führen in besonderem Maße zu einem Überwachungsproblem.

In Kombination der heute bereits existierenden Softwarelösung Google Earth sowie moderner Ortungstechnik (GPS im Armband) lassen sich z.B. in naher Zukunft vielleicht Kinder in Echtzeit orten und auf dem Weg zur Schule beobachten.[373] Während sowohl der intelligente Rahmen in Abbildung 13 als auch die Ortung durchaus spannende und sicherlich nachgefragte Services einer zukünftigen UC-Welt sein könnten, stellt sich in beiden Beispielen bei kritischer Reflektion die Frage nach der informationellen Selbstbestimmung und dem Datenschutz des Beobachteten: Wer sollte auf wen und unter welchen Umständen zugreifen können? Wie kann hier durch entsprechende Kontrollen auf Seiten des Beobachteten sichergestellt werden, dass informationelle Selbstbestimmung immer gewährleistet ist? Wann sollen Ausnahmen bestehen dürfen? Sollen diese Trackinginformationen gespeichert werden? Und wenn ja, von wem und für wie lange? Kapitel 6 dieser Studie geht aus juristischer Sicht auf diese Fragen ein.

Sicherlich sind ökonomische Anreize denkbar, welche für eine bewusste Einschränkung von Freiheiten der Beobachteten sprechen. Man denke z.B. an Unternehmen, die ihren Außendienst jederzeit orten wollen, um die Effizienz von Mitarbeitern prüfen zu können. Ebenso könnte die permanente Überwachung von Anlagen, Herstellungsprozessen, Gebäudemonitoring usw. dazu genutzt werden, Mitarbeiter indirekt zu überwachen: Bei welchen Schichten gab es den meisten Ausschuss? Wie häufig geht ein Mitarbeiter in die Zigarettenpause? Wer verbraucht den meisten Strom? All dies sind Fragen, auf deren Beantwortung ein Unternehmen im Regelfall verzichten mag, es jedoch Fälle geben kann, in denen ein Rückgriff auf die entsprechenden Informationen erfolgt. Von daher stellt sich die Frage, welche gesetzlichen Grenzen hier bereits existieren oder noch erforderlich sind.

Ein weiterer ökonomischer Anreiz besteht in der permanenten Überwachung von menschlichem Verhalten zum Zwecke der individuellen Bepreisung von Gütern und Dienstleistungen.[374] Ein Beispiel hierfür ist der an der ETH Zürich entwickelte „Smart Tachograph“.[375] Die-

[373] Google Earth nutzt keine Echtzeitbilder, u.a. da dies nach dem bisherigen Stand der Technik nicht möglich ist. Eine Markierung von Personen in regelmäßig aktualisierten Standbildern ist jedoch denkbar.

[374] Welzel / Filipova: Reducing Asymmetric Information in Insurance Markets: Cars with Black Boxes, Volkswirtschaftliche Diskussionsreihe, U. A. Institut für Volkswirtschaftslehre, Augsburg, 2005.

[375] http://www.vs.inf.ethz.ch/res/show.html?what=tachograph (29.03.2006).

ses Gerät zeichnet mittels Sensoren das Fahrverhalten eines Fahrers auf und berechnet in Abhängigkeit von Geschwindigkeitseinhaltung, Bremsverhalten, Abstandseinhaltung und Tageszeit in welchem Maß der Fahrer einen gesetzeskonformen und sicheren Fahrstil einhält. Weicht er negativ von der Norm ab, so soll sich seine Versicherungsprämie erhöhen.

Problematisch ist bei dieser Art Dienst nicht nur, dass Menschen permanent beobachtet und dadurch gezwungen werden, sich möglichst konform zu verhalten. Auch wirft individuelle Bepreisung Fragen der Solidarität und Gerechtigkeit auf. Auf den ersten Blick scheint es gerecht, jemanden für schlechtes Fahrverhalten mit einer höheren Prämie „zu bestrafen". Jedoch mag es Situationen geben, in denen schnelles Fahren angebracht ist. Und möglicherweise spielen auch die Straßenverhältnisse und Wohngegend eines Fahrers eine Rolle bei der Einschätzung, wann es sicher ist, in der einen oder anderen Weise zu fahren. Auf den zweiten Blick erscheint die Frage nach der Fairness und dem Sinn einer individuellen Bepreisung daher komplexer. Noch schwieriger wird ihre Beantwortung, wenn man sensible Lebensbereiche betrachtet, an denen eine Person nichts ändern kann: Sollte man beispielsweise Menschen auch für ihren Gesundheitszustand individuell zur Kasse bitten? Sollte man ihre Kreditwürdigkeit pauschal ermitteln?

Schon heute gibt es Ansätze eines individualisierten Umgangs mit Kunden, etwa durch das Kreditscoring. In vielen Firmen wird bereits regelmäßig eine Umsatzsegmentierung von Kunden vorgenommen, um das individuelle Servicelevel zu determinieren. In vielen Bereichen, in denen es nicht das unmittelbare Verhalten ist, welches zur Beurteilung führt, sondern die körperlichen Schwächen und sozialen Verhältnisse eines Menschen, wirft Individualisierung von Preisen und Dienstleistungen die Frage danach auf, was wir als Gesellschaft noch für menschenwürdig und gerecht halten. Die unten dargestellten Ergebnisse der empirischen Studie enthalten einige spannende Erkenntnisse zu diesem Sachverhalt.

Schließlich stellt die Personalisierung und Verbesserung von Angeboten und Vertriebskanälen einen hohen Anreiz dar, Kunden bei ihren Kaufentscheidungen zu beobachten. Bereits heute wird dies im E-Commerce im Internet, zum Beispiel mit Hilfe des „Mining" von Klickverläufen regelmäßig praktiziert. In UC-Umgebungen könnte für Unternehmen beispielsweise das Scannen von RFID-Chips am Körper eines Passanten aufschlussreich darüber sein, für welche anderen Produkte sich dieser interessiert. Eine Einkaufspassage könnte ihm oder ihr dann individuelle Werbung zeigen (siehe Szenarien).[376] Auch hier lässt der gebotene Service einen hohen Attraktivitätsgrad erwarten. Die Frage, die sich stellt ist, welche Wahl dem Kunden überlassen wird: Wird er gezwungen, der Werbung seine Aufmerksamkeit zu schenken oder kann er diese abschalten? Oder umgekehrt: Sollte es zunächst gar keine Werbung geben, diese jedoch bei Interesse abrufbar sein? Wie sollten die Standardvoreinstellungen (zu Englisch „Default Settings") hier aussehen? Wie akzeptiert ist eine Personalisierung, die auch zu Ausgrenzung führen kann? Und wie viel Kontrolle soll dem Kunden über RFID-Chips in seiner Kleidung obliegen, welche eine Erkennung und Einordnung dieserart überhaupt erst ermöglichen? Soll es überhaupt RFID-Chips geben, die im Laden und nach dem

[376] Smarter Retailing: Innovation at the Edge of the Retail Enterprise, Microsoft, 2004.

Kauf aktiv nutzbar sind, um solche Szenarien realistisch zu machen? Sollte vielleicht eine RFID-Schutztechnologie genutzt werden, um Services zu ermöglichen? In den folgenden Abschnitten dieses Kapitels soll auf diese Fragen näher eingegangen werden.

Auch zwischenmenschliche (soziale) Motive sind denkbar, durch die es zu einer fragwürdigen Ausnutzung der Technik kommen könnte. Denkbar ist hier beispielsweise ein überzogenes Kontrollbedürfnis von Partnern, Eltern, Arbeitgebern oder anderen Personen, die von anderen einen „Always on"-Zustand erwarten. Eine solche Erwartungshaltung kann heute bereits im Umgang mit Mobiltelefonen beobachtet werden. Auch ist nicht auszuschließen, dass ein sozialer Druck entsteht, zum Beispiel zwischen Jugendlichen, die das gegenseitige „Chipping" zum Kultstatus erheben.

Schließlich gibt es auch offene Fragen an der Schnittstelle zwischen Bürger und Staat. Selbstverständlich erlaubt es die UC-Technologie durch Remote Access-Anwendungen auch staatlichen Stellen, auf mehr Informationen über Bürger zuzugreifen. Überwachungsmaßnahmen zur Kriminalitäts- und Terrorbekämpfung führen zu einer erhöhten Datensammlung und -speicherung. Auf diese Daten könnten feingranulare Segmentierungs- und Prognoseverfahren angewendet werden, die für jeden Bürger eine Kriminalitätswahrscheinlichkeit ermitteln, Unregelmäßigkeiten in Prozessen im öffentlichen Raum erkennen oder auch einfach die Fahndung vereinfachen. Das aus heutiger Sicht futuristische Konzept der „Digital Bubble" sieht vor, an Orten des Verbrechens pauschal alle angefallenen Informationen unterschiedlichster Quellen für ein Zeitfenster zu aggregieren, um das Geschehen möglichst detailliert nachzuvollziehen.[377] Solche Anwendungen führen dazu, dass Bürger gegenüber dem Staat an vielen Stellen gläsern werden, auch solche, die mit Verbrechen nichts zu tun haben; eine Entwicklung, die die SWAMI-Gruppe als „individual transparent, power opaque" beschreibt (zu Deutsch: „transparentes Individuum, undurchsichtige Macht").

Die große Menge an Fragen zeigt, dass die Überwachungsmöglichkeiten des UC durch Remote Access-Anwendungen eine gesellschaftspolitische Debatte von großer Komplexität erzeugen. Ziel dieses Berichts kann es nicht sein, die anfallenden Fragen für die Gesellschaft zu klären. Interessant und wichtig ist jedoch, ein Gefühl dafür zu gewinnen, welche Meinung in der Bevölkerung zu UC-Anwendungen und zum Datenschutz besteht und wo diese Meinung kritischer Natur ist. International gelten die Deutschen als sehr sensibel was den Datenschutz betrifft. Trotzdem geht auch hierzulande das Datenschutzbewusstsein nicht immer mit einem konformen Schutzverhalten einher.[378]

5.3.1 Wahrnehmung des Privacy-Risikos in UC-Szenarien

Die obigen Ausführungen zeigen, dass Überwachung, Datenschutz und informationelle

[377] In Beslay / Hakala: Digital Territory: Bubbles, http://europa.eu.int/information_society/topics/research/visionbook/index_en.htm (29.03.2006).

[378] Berendt / Guenther et al.: Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, Communications of the ACM 48(4), 2005.

Selbstbestimmung zentrale Themen bei UC-Szenarien sein können, insbesondere wenn es um Remote Access-Anwendungen geht.

Aus diesem Grund wurden die Teilnehmer der empirischen Studie nach ihrer Einschätzung befragt, für wie hoch sie das Risiko halten, dass ihre Privatsphäre durch eines der vier UC-Szenarien beeinträchtigt werden könnte. Dabei hat sich zunächst gezeigt, dass es einen signifikanten Unterschied in der Beurteilung zwischen denjenigen gibt, die sich online an der Befragung beteiligt haben und solchen, die auf Papier mitgemacht haben. Die deutlich höher gebildeten und online-affinen, überwiegend männlichen Teilnehmer der Internetbefragung schätzen das durch UC-Services entstehende Privacy-Risiko als signifikant höher ein als die Teilnehmer der Papierstudie. Da die Papierstudie jedoch in ihrer soziodemographischen Zusammensetzung deutlich repräsentativer für die deutsche Bevölkerung ist, wollen wir uns im Folgenden an vielen Stellen auf diese wenn auch kleinere Stichprobe fokussieren.

Es zeigt sich, dass das Privacy-Risiko gemischt wahrgenommen wird. Bei Heimapplikationen wie Kühlschrank und Arbeitsplatz ist es deutlich höher als beim Auto. Abbildung 14 macht dies deutlich. Hier zeigt sich, dass die Befragten den intelligenten Kühlschrank im Durchschnitt für ein mittleres bis eher höheres Privacy-Risiko halten (54% sehen in ihm ein hohes oder sehr hohes Privacy-Risiko). Bei der intelligenten Wartung ist dieser Durchschnitt signifikant geringer (gerade einmal 31,4 % empfinden ein hohes oder sehr hohes Privacy Risiko). Der Vergleich der beiden Anwendungen ist vor dem Hintergrund interessant, dass beide Services in ähnlicher Form Zustände beobachten (leerer Kühlschrank, defekte Wagenteile) und dann eine Bestellung an einen externen Dienstleister auslösen. Trotzdem führt das Szenario Kühlschrankauffüllung zu einer kritischeren Einschätzung als das Szenario Autowartung. Das Ergebnis könnte auf die naheliegende Vermutung hindeuten, dass die Wahrnehmung von Privacy-Risiken für heimische UC-Dienste (Küche) höher ist, als dies für Anwendungen im öffentlichen Raum (Straße) der Fall ist. Dies ginge konform mit Arbeiten von Altmann, einem Privacy-Soziologen, der die unterschiedliche Bedeutung von Privatsphäre für öffentliche und private Orte beschreibt.[379] Es könnte jedoch auch argumentiert werden, dass beim Kühlschrank Verhalten beobachtet wird, nämlich Lebensmittelverbrauch, während es bei der Wartung nicht um Verhalten, sondern lediglich um den Zustand des Objekts Auto geht. Vor diesem Hintergrund wäre dann jedoch auch eine kritischere Beobachtung des Fahr*verhaltens* zu Bremszwecken naheliegend gewesen.

Ferner zeigt sich, dass der Arbeitsplatz mit dem größten Privacy-Risiko verknüpft ist. Diese Beobachtung könnte darauf zurückzuführen sein, dass Privacy-Risiken heute häufig im Kontext der modernen Datenverarbeitung diskutiert werden.

[379] Altman: The environment and social behavior: Privacy, personal space, territory, crowding, Monterey, California, Brooks/Cole, 1975.

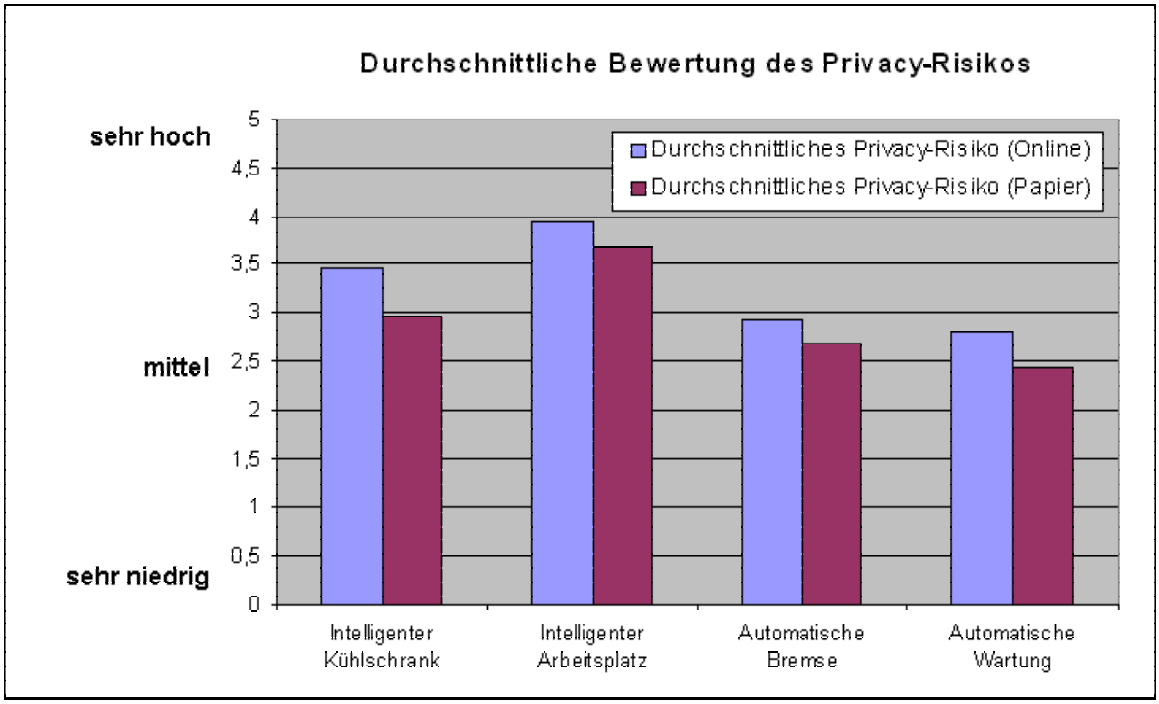


Abbildung 14: Beurteilung des Privacy-Risikos der vier UC-Szenarien

5.3.2 Relative Bedeutung von Privacy-Risiken bei der UC-Akzeptanz

Die Wahrnehmung des Privacy-Risikos allein ist nicht aussagekräftig genug, um auf die Rolle von Privacy für die Akzeptanz von UC-Szenarien schließen zu können. Eine weiter gehende Analyse zeigt zwar, dass das empfundene Privacy-Risiko einen Einfluss auf die oben bereits diskutierte affektive Bewertung eines UC-Szenarios hat. Allerdings zeigt sich vor dem Hintergrund der vier untersuchten Szenarien, dass dieser Einfluss relativ geringer ist als andere Faktoren, wie etwa das Vertrauen in den Dienst, Kontrolle oder etwa das psychosoziale Risiko, dass ein Dienst nicht in den Alltag passen könnte. Abbildung 15 verdeutlicht dies. Hier zeigt sich, dass das Privacy-Risiko für die Einschätzung der Nützlichkeit kaum eine Rolle spielt. Bei Betrachtung der Einflussstärke von Privacy pro Szenario (für Details siehe Appendix 7) sieht man, dass Privacy-Bedenken noch am ehesten im Auto auf die Einschätzung der Nützlichkeit wirken. Naheliegend ist, dass die Teilnehmer der Papierstudie es als ihre Privatangelegenheit begreifen, ob sie bremsen und wie sie ihren Wagen warten. Durchgängig lässt sich für alle Szenarien und beide Stichproben nachweisen, dass ein erhöhtes Privacy-Risiko zu einer Reduzierung der Freude an der Applikation führt (affektive Bewertung), dass dieser Einfluss allerdings relativ schwächer ist als andere Faktoren. Und dass schließlich Privacy-Risiken nicht direkt die Kauf- oder Nutzungsintention beeinflussen. Diese Ergebnisse legen nahe, dass dem wahrgenommenen Privacy-Risiko allein eine geringere Bedeutung für die Beurteilung von UC-Szenarien zukommt als anderen Entscheidungsfaktoren.

Dies entspricht auch dem gegenwärtigen Stand der Privacy-Forschung, wo man immer wieder beobachtet, dass die Wahrnehmung von Privacy-Risiken und die Privacy-Einstellungen nicht in der Lage sind, Verhalten zu erklären. Offensichtlich gibt es andere Faktoren, wie

etwa das Vertrauen in ein System, welches eine höhere Handlungsrelevanz besitzt. In der Literatur geht man davon aus, dass Menschen Kosten/Nutzenabwägungen durchlaufen, wenn sie sich für die Preisgabe von Informationen entscheiden. Dabei zeigt sich, dass der kurzfristige Nutzen sehr häufig höher bewertet wird als der hypothetische langfristige Schaden aus einer Datenpreisgabe.[380] Die meisten Menschen entscheiden sich also trotz Privacy-Bedenken dafür, dass Daten erhoben werden, um von unmittelbaren Vorteilen zu profitieren. Selbstverständlich spielt in diesem Kalkül die Kostenfunktion des Betroffenen eine wichtige Rolle: Erwartet er einen geringen Schaden aus der Verletzung von Privatsphäre (z.B. weil er in das Gesetz vertraut) oder schätzt er diesen Schaden als unwahrscheinlich ein, so macht es wenig Sinn für ihn, auf die meist unmittelbaren Vorteile der Datenpreisgabe zu verzichten. Der anschließende Abschnitt wird auf diesen Aspekt näher eingehen und untersuchen, inwieweit die Teilnehmer der Studie Kosten bzw. Schaden durch ihre Datenpreisgabe in Deutschland erwarten.

Berücksichtigt werde sollte jedoch noch, dass das hier gemessene Privacy-Risiko und die wahrgenommene Kontrolle durchgängig eine mittlere Korrelation aufweisen. Dies bedeutet wiederum, dass obgleich das Privacy-Risiko allein wenig bedeutsam ist, es über die wahrgenommene Kontrolle doch einen Einfluss auf die Wahrnehmung des UC-Service ausübt (siehe Appendix 10).

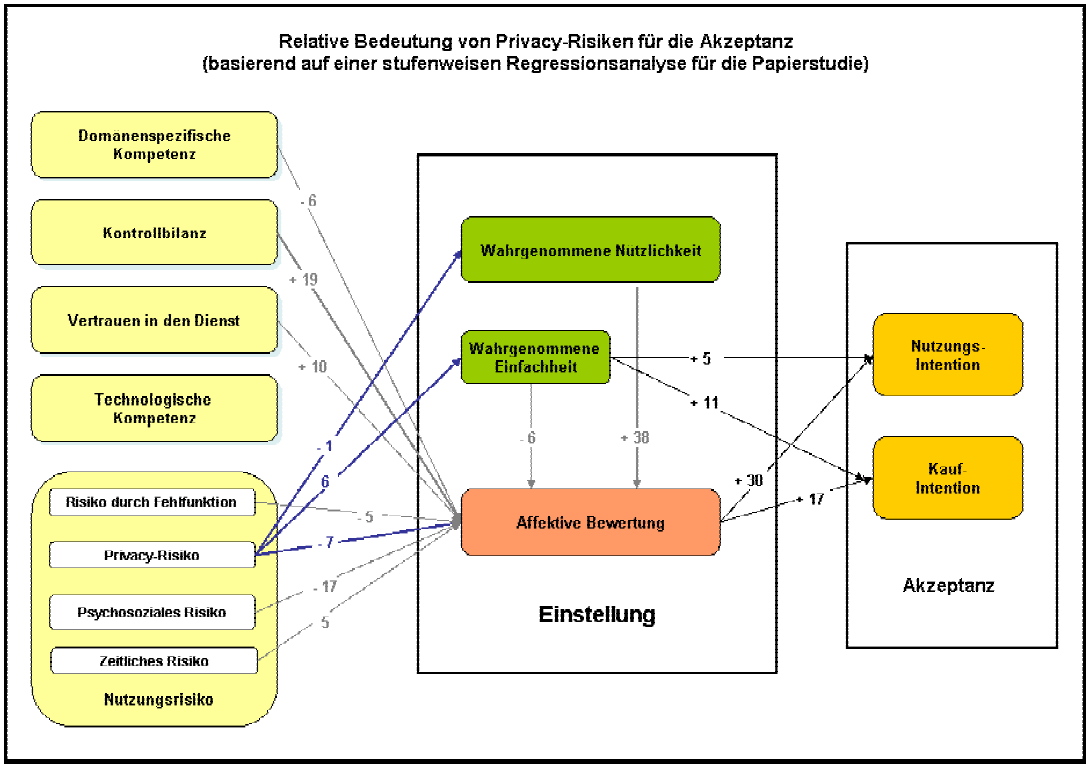


Abbildung 15: Bedeutung des Privacy-Risikos und anderer Faktoren für die emotionale Reaktion auf ein UC-Szenario (nur Papierstudie)

[380] Acquisti / Grossklags: Privacy and Rationality in Individual Decision Making, IEEE Security & Privacy. 2, 2005, S. 24-30.

5.3.3 Bedeutung und Wahrnehmung von Datenschutz

Geht man der Frage nach, ob UC-Technologien an einem zu hohen Datenschutzbewusstsein von Verbrauchern scheitern könnten, so reicht es nicht, diese danach zu fragen, inwieweit sie ihre Privatsphäre durch UC-Technologien bedroht sehen. Wie oben bereits gezeigt, können Verbraucher ein ausgeprägtes Bewusstsein für ein Privacy-Risiko haben. Entscheidend ist jedoch, wie handlungsrelevant dieses Bewusstsein ist. Wird man UC-Services aufgrund von Datenschutzbedenken bewusst nicht nutzen und nicht kaufen, wenn deren Nützlichkeit gleichzeitig hoch ist?

Entscheidend für die Beantwortung dieser Frage ist zu verstehen, welche „Kosten" bzw. negativen Auswirkungen Verbraucher durch die Nutzung von UC-Services erwarten. Fühlen sich Verbraucher durch Datenschutzgesetze ausreichend geschützt, so vertrauen sie auf gesetzeskonforme Abläufe. Glauben Verbraucher, dass mit den gesammelten Daten ohnehin wenig „gemacht" wird oder dass ihre Daten wenig aussagefähig sind, so haben sie auch kein Problem damit, diese weiterzugeben; auch nicht in einem UC-Umfeld.

Vor diesem Hintergrund werden die Teilnehmer der Studie nach ihren Vorstellungen vom gesetzlichen Datenschutz in Deutschland befragt, nach dem ihnen bewussten Grad der Überwachung und nach ihren Vorstellungen von der Datenverarbeitung. Die folgenden Abschnitte geben die hier gesammelten Erkenntnisse wieder. Dabei wird der kritische Leser konstatieren, dass die Teilnehmer hier nach dem gegenwärtigen Schutz- und Datenverarbeitungsniveau befragt wurden. Es handelt sich also um eine Momentaufnahme des Wissens und der Einstellungen zum Datenschutz in einer Zeit, in der noch deutlich weniger Daten erhoben werden, als dies in einer zukünftigen UC-Umgebung zu erwarten ist. Diese Vorgehensweise liegt darin begründet, dass es für die Befragten leichter ist, ihr Wissen und ihre Vorstellungen von etwas zu formulieren, was sie schon kennen. Bereits heute wird durch Kundenkarten, Internet, Telefon- und Videoüberwachung eine ständig steigende Menge an persönlichen Daten erhoben, zum Teil auch schon durch UC-Anwendungen. Ist die Bevölkerung kritisch ob dieser Entwicklungen, so könnte man erwarten, dass sich dies durch Ubiquitous Computing weiter verschärft. Leider gibt es derzeit keine empirisch validen Erkenntnisse zu diesem Sachzusammenhang. Stattdessen wird gerne argumentiert, dass die breite Akzeptanz von Kundenkarten und die damit verbundene Verarbeitung von Daten ein Indiz dafür sind, dass die kommerzielle Datenverarbeitung aus Kundensicht generell in Ordnung ist. Die durchgeführte Befragung hatte u.a. das Ziel zu untersuchen, ob und vor welchem Wissenshintergrund dies tatsächlich der Fall ist.

5.3.3.1 Wahrnehmung von Datenschutzgesetzen und Datenverarbeitung in Deutschland

Bei der Untersuchung der Wahrnehmung des deutschen Datenschutzniveaus durch Gesetze zeigt sich, ähnlich wie in oben genannten Analysen, ein signifikanter Unterschied zwischen den online Befragten und den Teilnehmern der Papierstudie, wobei wir noch einmal darauf hinweisen möchten, dass die Papierstudie zwar kleiner (n=200), dafür aber deutlich repräsentativer für die deutsche Bevölkerung ist. Laut Papierstudie fühlen sich 68 % der Befragten

zumindest ausreichend durch Datenschutzgesetzte geschützt, während es bei den Internetbefragten deutlich weniger sind, nämlich nur noch 49 %.

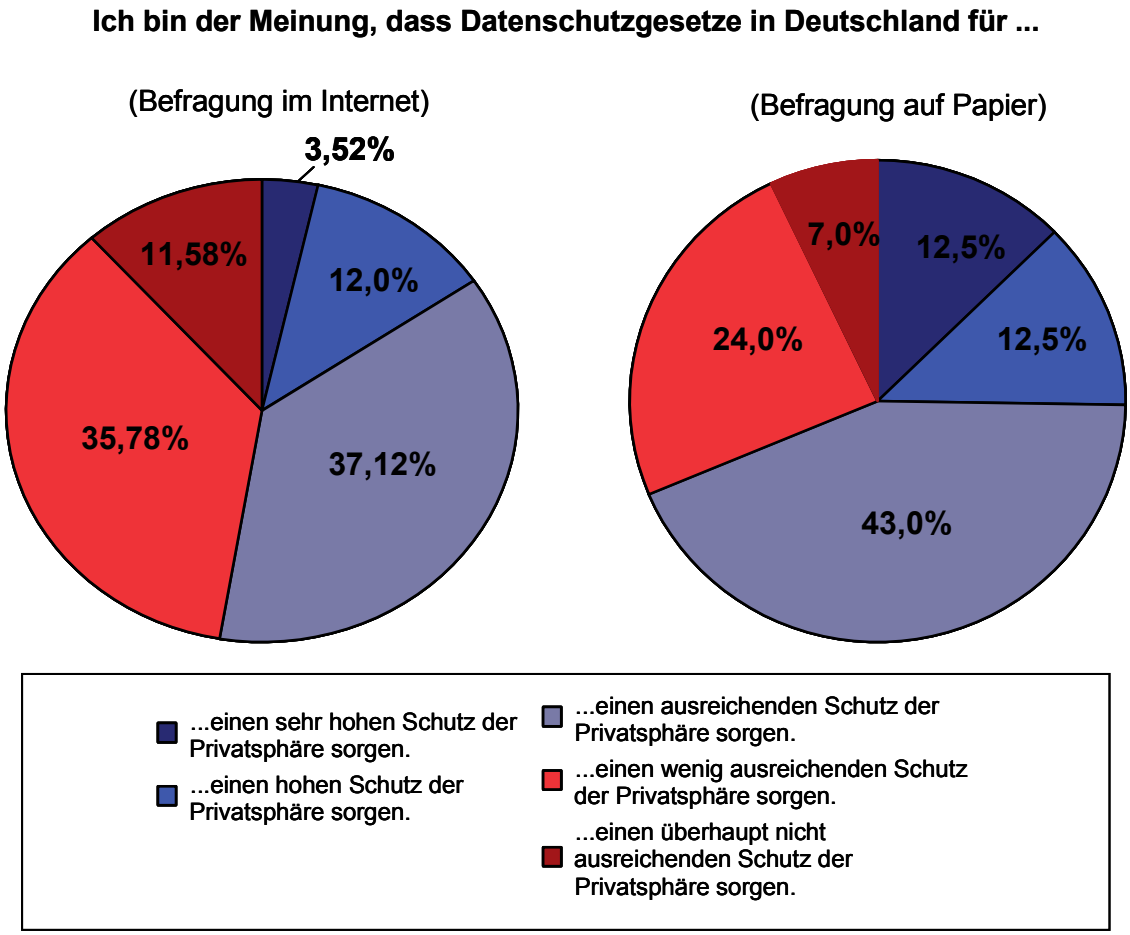


Abbildung 16: Wahrnehmung des Schutzniveaus durch deutsche Datenschutzgesetze

Bei den online Befragten mag diese kritischere Bewertung des Datenschutzniveaus teilweise darauf zurückzuführen sein, dass hier der Mehrheit der Teilnehmer (61 %) bewusst ist, dass ein Missbrauch von Kundendaten in Deutschland mit relativ wenigen Sanktionen für Unternehmen verbunden ist (siehe Abbildung 16 links).

Diese Daten legen nahe, dass es in Deutschland ein relativ hohes Vertrauen in die Gesetzeslandschaft gibt, dass dieses jedoch signifikant abnimmt, wenn Menschen bewusst wird, dass Gesetzesverstöße tatsächlich mit wenigen Sanktionen für Unternehmen verbunden sind. Abbildung 16 veranschaulicht dies weiter: Schaut man sich nur solche online Befragten an (60,5 %), denen das geringe Sanktionsniveau bewusst ist, so fällt der Anteil der in Gesetze Vertrauenden von 52,6 % auf 37,9 %.

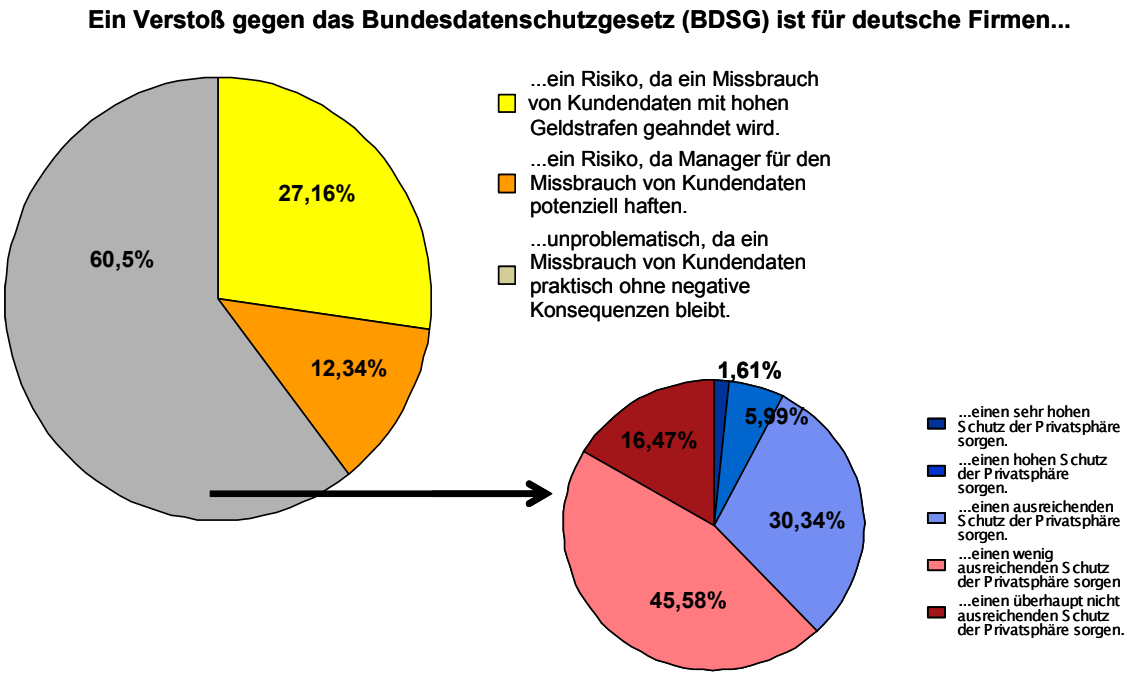


Abbildung 17: Wahrnehmung des Schutzniveaus bei aufgeklärten Bürgern (nur online Befragte)

Ebenso schätzen die Befragten online und auch auf Papier die Überwachungsdichte als deutlich geringer ein, als dies tatsächlich der Fall ist. Die Teilnehmer wurden im Rahmen der Befragung aufgefordert zu schätzen, wie viele Personen in Deutschland jedes Jahr von Telefonüberwachung betroffen sind. Ebenso wurden sie aufgefordert zu schätzen, wie viele Videokameras in England für die Überwachung öffentlicher Plätze eingesetzt werden. Der geschätzte Median der Telefonüberwachung liegt bei 10.000 betroffenen Personen. Tatsächlich gibt es in Deutschland jedoch im Jahr ca. 30.000 Anordnungen zur Telefonüberwachung.[381] Nimmt man an, dass von jeder Anordnung im Schnitt sechs Personen betroffen sind, so hätte eine realistische Schätzung bei ca. 200.000 liegen müssen. Abbildung 17 visualisiert, dass damit über 80% der Befragten den Grad der Telefonüberwachung in Deutschland unterschätzen.

Der gleiche Trend findet sich auch in der Schätzung der Anzahl der Videokameras für das Vereinigte Königreich wieder. Auch hier liegt der Median bei 10.000 Kameras. Laut Schätzungen einer Studie aus dem Jahr 2002 soll das sog. „CCTV“ in dem Vereinigten Königreich jedoch rund vier Millionen Kameras umfassen.[382]

Diese Befragungsergebnisse legen nahe, dass die gegenwärtige Überwachungsdichte stark unterschätzt wird.

[381] Bundesregierung, BT-Drs. 15/4011, S. 6: 29 438 Anordnungen, BT-Drs. 15/6009, S. 10: 34 374 Anordnungen.

[382] CCTV steht für „Closed-circuit television“. Die Schätzungen sind auf eine 2002 Studie im Rahmen des 5. Europäischen Rahmenprogramms durch das Centre for Criminology and Criminal Justice zurückzuführen McCahill / Norris: CCTV in London, C. f. C. a. C. Justice, Hull, UK, 2002.

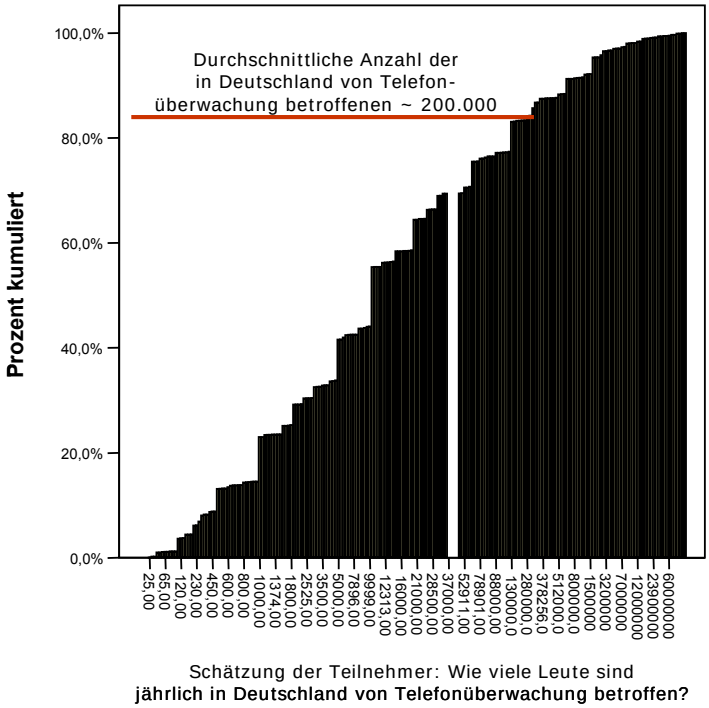


Abbildung 18: Schätzung der Telefonüberwachungsdichte in Deutschland

5.3.3.2 Wissen um die kommerzielle Datenverarbeitung

Deutlich aufgeklärter zeigen sich die Befragten hingegen bei der Einschätzung der Datenverwertung durch Unternehmen. Über 70% der Befragten auf Papier und über 90% der online Befragten gehen davon aus, dass Supermärkte die Einkaufsdaten ihrer Kunden regelmäßig auswerten. Den meisten ist bewusst, dass ihre Einkaufsdaten nicht lokal beim Supermarkt verbleiben, sondern an andere verarbeitende Stellen weitergeleitet werden (siehe Abbildung 19). Allerdings zeigt sich auch hier wieder ein signifikanter Unterschied zwischen der Papier- und Onlinestichprobe. Gehen von den online Befragten 75 % davon aus, dass Einkaufsdaten noch an mindestens drei weitere Stellen in Deutschland weitergeleitet werden, so sind es bei den auf Papier Befragten nur 61 % und der Anteil der Unentschlossenen ist mit 22 % hier fast doppelt so hoch wie bei den online Befragten (13 %).

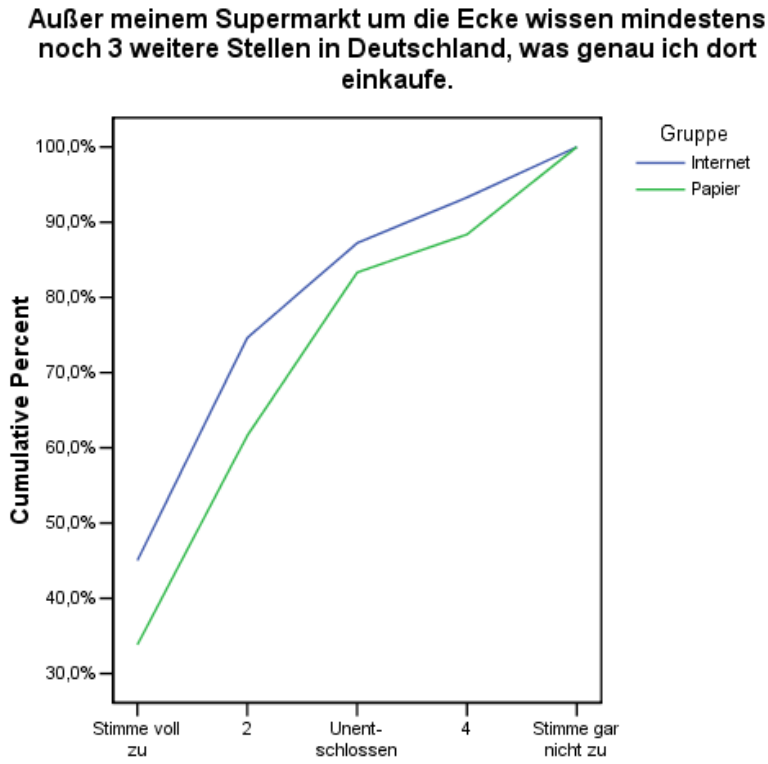


Abbildung 19: Erwartung an die Weiterleitung von Daten durch kommerzielle Entitäten (Fall Supermarkt)

Umgekehrt könnte man auch sagen, dass sich bei der repräsentativeren Papierbefragung rund 40 % der Teilnehmer als „Unwissende“ herausstellen was die Weiterleitung von Einkaufsinformationen angeht. Diese Zahl spiegelt sich auch in der Frage danach wieder, ob Teilnehmer glauben, dass ihre Einkaufsdaten in der Masse der Daten anderer untergehen. Dies können sich 40 % der auf Papier Befragten durchaus vorstellen. 38,2 % der auf Papier Befragten gehen auch davon aus, dass ihre Einkaufsdaten gelöscht werden, wenn ein Supermarkt pleite geht und 37 % glauben, dass heute gesammelte Einkaufsdaten in fünf Jahren niemanden mehr interessieren (oder sind zumindest unentschlossen). Allerdings trifft der Glaube an die Örtlichkeit von Daten, deren Vergänglichkeit und Untergehen in der Masse in Kombination nur bei 28 % der auf Papier Befragten zu (sowie auf 15 % der online Befragten)[383]. 61% dieser Leute besitzen eine Kundenkarte. Diese Zahl ist von Bedeutung, da der Anteil der Kundenkartenbesitzer für die untersuchte Gesamtpopulation bei nur 38 % liegt. Dies deutet darauf hin, dass Personen, die weniger über die Datenverarbeitung wissen, eher bereit sind, von Services zu profitieren, die ihre Privatsphäre potenziell beeinträchtigen könnten.

Zusammenfassend lässt sich sagen, dass die Mehrheit der Befragten die kommerzielle Datenverarbeitung durchaus realistisch einschätzt. Allerdings gibt es einen robusten Anteil der Bevölkerung von möglicherweise 25 – 40 %, bei denen dies nicht so ist. Hier besteht dann

[383] Hier wurde die Kombination der Fragen zur Weiterleitung an 3 weitere Verarbeitungsstellen, zum Untergehen in der Masse und zum Interesse an Daten 5 Jahre später zugrunde gelegt.

tendenziell weniger Vorsicht in der Nutzung informationsintensiver Dienstleistungen. Umgekehrt kann auch nicht ausgeschlossen werden, dass mehr Wissen über die Datenverarbeitung zu einem zurückhaltenderen Umgang mit informationsintensiven Dienstleistungen führt. Diese Erkenntnis ist für die Gestaltung von UC-Services bedeutend.

5.3.3.3 Beurteilung der Datennutzung

Um beurteilen zu können, welchen potenziellen Schaden bzw. welche „Kosten" Verbraucher durch die Verarbeitung ihrer Daten erwarten, reicht es nicht aus zu wissen, was sie von der Datenverarbeitung wissen, sondern auch inwieweit sie einen Schaden erwarten. Die Teilnehmer wurden zu diesem Zweck befragt, inwieweit sie glauben, dass ihre Einkaufsdaten in einem Rechtsstreit beweiskräftig sein können. Es zeigt sich, dass hier die meisten Befragten (81%) selbst in der eher kritischen und gut informierten Onlinestichprobe unentschlossen sind (48 %) oder nicht glauben, dass ihre Einkaufsdaten Beweiskraft haben (33 %). 62% der auf Papier Befragten glauben ferner, dass es ihnen kaum schaden kann, wenn andere wissen, was man täglich verbraucht. Diese Ergebnisse sprechen dafür, dass eine Mehrheit der Befragten nicht davon ausgeht, dass Informationen, die über sie gesammelt werden, gegen sie verwendet werden können.

Zu diesem Ergebnis passen inhaltlich auch die moralisch ethischen Erwartungen, die die Befragten der vorliegenden Studie an Unternehmen haben, wenn es um die Nutzung von Informationen im Umgang mit Kunden geht. Die Teilnehmer wurden befragt, ob sie es in Ordnung finden, wenn sie hören, dass ein Freund in der Warteschlange eines Mobilfunkbetreibers länger warten muss als andere Kunden, da er ein schlechterer Kunde ist. 90,4 % der Befragten der Gesamtstichprobe finden solch einen Umgang mit Kunden nicht in Ordnung oder gar nicht in Ordnung. Und selbst wenn man nur die relativ besser Verdienenden betrachtet (mit einem monatlichen Nettoeinkommen von über € 2.000), so sind es immer noch 87 %, die ein solches Verhalten von Unternehmen nicht in Ordnung finden (siehe Abbildung 17 links). Noch kritischer ist die Einschätzung, wenn es sich darum handelt, dass jemand möglicherweise nicht mehr per Kreditkarte im Internet bezahlen kann, da er in einem Stadtviertel wohnt, in dem viele Leute Schulden haben und die Kreditwürdigkeit an der Nachbarschaft festgemacht wird. 96 % der Gesamtstichprobe finden so ein Verhalten von Firmen nicht in Ordnung oder gar nicht in Ordnung. Nimmt man nur die besser Verdienenden bleiben es immer noch 96 % (siehe Abbildung 17 rechts).

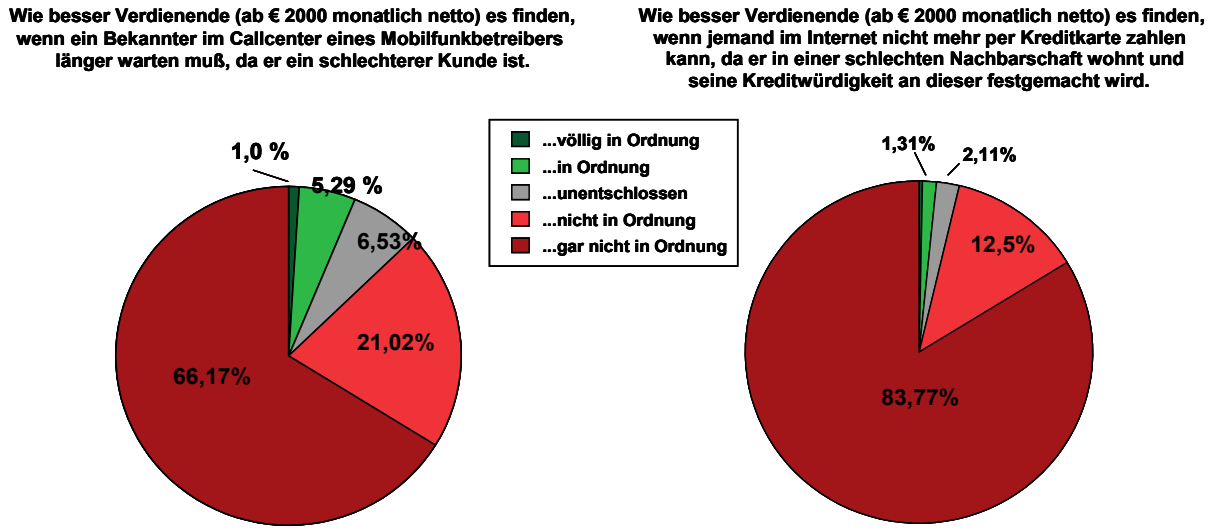


Abbildung 20: Bewertung von ökonomisch sinnvoller personalisierter Kundenbetreuung, die jedoch mit negativen Auswirkungen für den Einzelnen verbunden ist (beide Stichproben kombiniert)

Diese Erkenntnisse sprechen insgesamt dafür, dass Verbraucher moralisch hohe Erwartungen an Unternehmen im Umgang mit Kundendaten haben. Eine Diskriminierung von Kunden ist nicht gewünscht. Insbesondere dann nicht, wenn sich die Diskriminierung an selbst nicht beeinflussbaren (oder nur schwer beeinflussbaren) Kriterien festmacht, wie etwa der Wohngegend. Die Zahlen zur Beurteilung von diskriminierender Datennutzung legen nahe, dass Firmen bereits heute ein Risiko eingehen, wenn sie Kunden nach ihrem Umsatz, Verhalten oder anderen Kriterien segmentieren und es als Folge davon zu einer als mehrheitlich unfair empfundenen Ungleichbehandlung kommt. Zumindest in den beiden abgefragten Fällen finden Kunden ein solches Verhalten nicht in Ordnung.[384]

Dies bedeutet nicht, dass Services wie etwa die oben beschriebene Versicherungsprämie nicht durchaus individuell tarifiert werden können, denn immerhin kann man bei der Versicherungsprämie immer noch den Preis durch das eigene Fahrverhalten beeinflussen. Etwaige Ungerechtigkeiten sind also selbst verschuldet. Ebenso gibt es in der Konsumentenforschung zur Preisgestaltung Hinweise darauf, was beachtet werden muss, damit Kunden ungleiche Preise akzeptieren.[385] Hier sei insbesondere auf die Transparenz und Fairness von Bepreisungsprozessen verwiesen.[386] Die Nutzung von UC-Technologie zur Optimierung ei-

[384] Diese Erkenntnis sollte in einer separaten Analyse vertieft werden, denn möglicherweise kann eine Umdrehung der Fragestellung zu einem differenzierteren Bild führen. Daher: Fragt man ‚bessere' Kunden, ob sie eine privilegierte Behandlung ihrer Person für gerechtfertigt halten, dann werden sie dies möglicherweise begrüßen. In der vorliegenden Abbildung 17 wird diese Argumentation berücksichtigt, indem nur die Ansicht der besser Verdienenden dargestellt wird, welche potenziell eher zu der Kundengruppe gehören, die von einer Ungleichbehandlung profitieren. Trotzdem ist eine tiefer gehende Analyse der Wahrnehmung von Differenzierungspraktiken erforderlich, um eine allgemein gültige Aussage machen zu können.

[385] Spiekermann: Individual Price Discrimination - An Impossibility, Berlin, Institute of Information Systems, Humbodlt University Berlin, 2005.

[386] Cox: Can differential prices be fair?, The Journal of Product and Brand Management 10(4), 2001, S. 264-276.

ner weitestgehend intransparenten Ungleichbehandlung allerdings sollte von Firmen vermieden werden, um einen „Privacy-Backlash“[387] zu vermeiden.

Insgesamt zeigt die bevölkerungsrepräsentative Befragung durch beide Medien, dass die Mehrheit der Deutschen einen hohen Schutz durch Gesetze empfindet, den Grad ihrer Überwachung unterschätzt, die kommerzielle Datenverarbeitung durchaus realistisch einschätzt, jedoch auch eine diskriminierende Nutzung von Informationen weder erwartet noch wünscht. Darüber hinaus legt die vorliegende Analyse nahe, dass es ein Segment von 25-40% der Bevölkerung gibt, welches keine realistische Vorstellung von der Datenverarbeitung hat und in Folge dieser „Naivität“ auch mit der Nutzung informationsintensiver Services großzügiger umgeht.

5.3.4 Wahrnehmung und Bewertung von Remote Access durch RFID-Technologie

Neben der hier beschriebenen BMBF-Studie (durchgeführt in Kooperation mit der Wochenzeitung DIE ZEIT) sei noch auf einige andere empirische Arbeiten verwiesen, die sich der Wahrnehmung und den Präferenzen von Remote Access-Anwendungen auf Seiten der Verbraucher gewidmet haben. Insbesondere wurde eine bereits oben erwähnte Studie zum Thema RFID und Privatsphäre im deutschen Einzelhandel durchgeführt, um potenzielle Bedenken von Verbrauchern zu verstehen und diesen begegnen zu können.[388] Im Rahmen dieser Studie wurden 30 Berliner Bürger in 4 Fokusgruppen über 4 x 2 Stunden hinweg beobachtet. Informationsgrundlage war ein positiv gestalteter Film der Metro Future Store Initiative über den Nutzen von RFID im Supermarkt der Zukunft (zu Beginn der Diskussion) sowie ein eher kritischer ARD-Bericht über die RFID-Technik und ihre Anwendungen (gegen Ende der Diskussion). Für Fragen stand ein neutraler Moderator zur Verfügung. Die Zusammensetzung der Gruppenteilnehmer entsprach ungefähr dem Bevölkerungsdurchschnitt in Alter, Bildung und Geschlecht. Ausgehend von den auf Tonband aufgenommenen und transkribierten Gesprächen konnten einige als wesentlich wahrgenommene Eingriffe in die Privatsphäre isoliert werden, welche in Kap. 5.4 zusammengefasst sind.

Bei Betrachtung der Fokusgruppenerkenntnisse zeigt sich, dass sich aus Sicht von Verbrauchern sechs Missbrauchsszenarien isolieren lassen. Die ersten drei beziehen sich dabei auf den Bereich der Überwachung, den die RFID-Technik auf verschiedene Weisen erlaubt. Der „entfernte Zugang“ (Remote Access) von Rechnerumgebungen (hier RFID-Lesegeräten) wird bei den Befragten – so scheint es auf Basis der Beobachtungen – als eine Verletzung ihrer Privatsphäre verstanden. Privatsphäre allerdings nicht nur im Sinne des oben diskutierten Datenschutzes und der Datenverarbeitung (Punkte 2 und 3 in Kap. 5.4), sondern auch im Sinne einer physischen Kontrolle und Transparenz dahingehend, wann man von wem zu

[387] The Economist: “The coming backlash in privacy”, 7. Dezember 2000, http://www.economist.com/displaystory.cfm?story_id=442790

[388] Berthold / Guenther et al.: RFID Verbraucherängste und Verbraucherschutz, Wirtschaftsinformatik Heft 6, 2005.; Guenther / Spiekermann: RFID and Perceived Control - The Consumer's View, Communications of the ACM 48(9), 2005, S. 73-76.

welchem Zweck durch RFID-Lesegeräte ausgelesen wird (Punkt 1). Überhaupt scheint das Konstrukt der Kontrolle über die Technologie ein wesentlicher Aspekt für die Einschätzung derselben durch Verbraucher zu sein. Dies zeigt sich auch in Zitaten wie:

> „…da wird mit mir was gemacht, was ich gar nicht so richtig kontrollieren kann und überblicken kann und das macht mir Angst."
>
> „Wer will das alles kontrollieren, dass die Daten nicht doch irgendwie noch anders verwendet werden. Wo ist da die Sicherheit gegeben?"

Diese Aussagen gehen mit den Ansichten von Fachleuten des Ubiquitous Computing einher. Ein „Urvater" des Ubiquitous Computing, Marc Weiser, stellte beispielsweise in einem seiner Grundsatzartikel zum Ubiquitous Computing fest, dass das wahre soziale Problem des Ubiquitous Computing, obgleich oft mit Privatsphäre umschrieben, wirklich das der Kontrolle ist.[389]

Die den Fokusgruppen nachfolgende experimentell variierte Befragung von 234 soziodemographisch repräsentativ ausgewählten Personen hat vor diesem Hintergrund untersucht, ob und durch welche Schutztechnologien (sog. „PETS" = Privacy Enhancing Technologies) Kunden ein Gefühl von Kontrolle über RFID vermittelt werden könnte.[390] Dazu wurden zwei Teilnehmergruppen gebildet, die auf Basis eines neutralen Films die RFID-Technologie beurteilen mussten. In jeder Gruppe waren RFID-Chips mit einer anderen Schutztechnologie versehen. Im ersten Film wurden RFID-Chips am Ladenausgang deaktiviert und mit einem Passwortschutz versehen (Passwort PET). Im zweiten Film wurden RFID-Chips am Ladenausgang zwar angelassen, jedoch mit einem Schutzmechanismus versehen, der nur autorisierten Lesegeräten einen Zugriff auf die Chips gewährt (Netzwerk PET).[391] Angenommen wurde, dass das Passwort PET beim Kunden zu einer größeren Kontrollwahrnehmung führt, da der Kunde dem Lesevorgang aktiv zustimmen muss.

Es hat sich jedoch gezeigt, dass beide Schutzvarianten von Kunden als gleichermaßen fragwürdig beurteilt werden. Abbildung 20 zeigt, dass die Teilnehmer der Studie bei beiden Schutzvarianten gleichermaßen ein Gefühl von Hilflosigkeit empfinden und das Gefühl haben, dass sie gegenüber der Technologie machtlos sind und keine Wahl haben. Gleichzeitig geben sie an, durchaus in der Lage zu sein, die Schutztechnologien zu bedienen, und auch ausreichend über den RFID-Lesevorgang informiert zu sein. Dabei bevorzugt die Mehrheit der Befragten (73%) die Vorstellung, dass RFID-Chips am Ladenausgang vollständig vernichtet werden (gekillt werden). Bei Teilnehmern mit Abitur waren es mit 78 % sogar noch einmal signifikant mehr, die diese kritische Haltung einnahmen. Und zu dieser kritischen Hal-

---

389 *„The [social] problem [associated with UC], while often couched in terms of privacy, is really one of control*." in: Weiser: The Computer for the 21st Century, Scientific American, 265, 1991, S. 94-104.

390 Auch hier gilt wieder zu beachten, dass es sich um keine statistisch repräsentative Befragung handelt, sondern um eine Schichtung von Experimentteilnehmern im Sinne einer Gewährleistung der Teilnahme von bevölkerungsrepräsentativen Gruppen.

391 Guenther / Spiekermann: RFID and Perceived Control - The Consumer's View, Communications of the ACM 48(9), 2005, S. 73-76.

tung gegenüber RFID kam es, obgleich, wie oben berichtet, die Mehrheit der Befragten die Nutzenvorteile von RFID durchaus sehen und begrüßen.

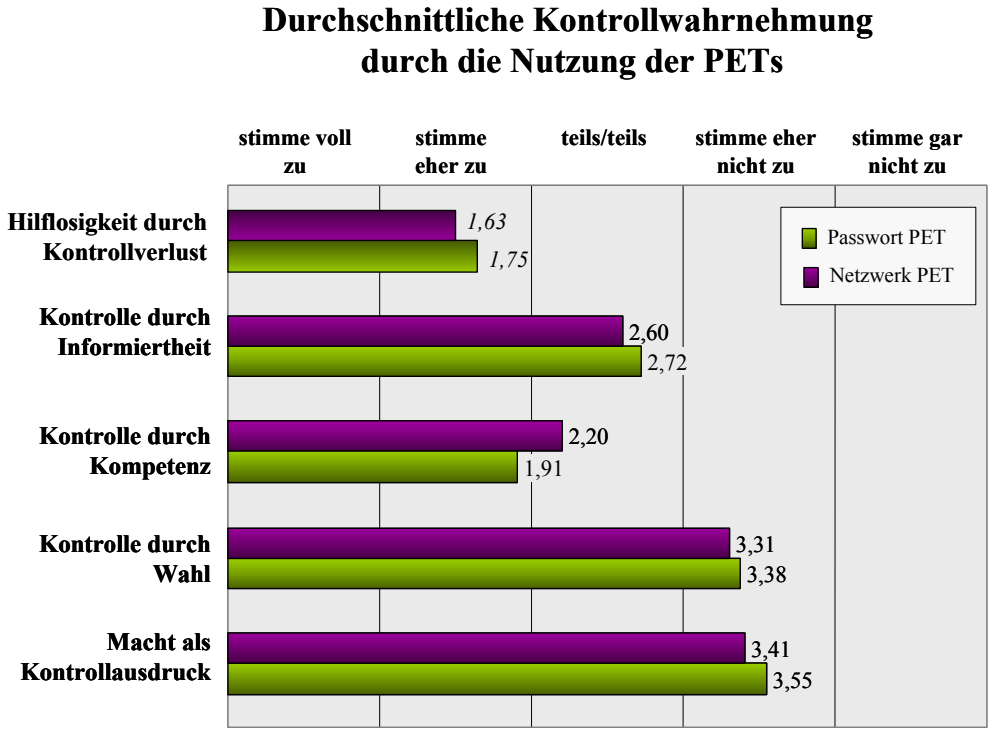


Abbildung 21: Kontrollwahrnehmung durch PETs

Diese Befunde deuten darauf hin, dass deutsche Verbraucher den Einsatz von RFID-Technologie auf Einzelproduktebene als sehr sensibel einstufen und dass es schwer ist, ihnen ein Vertrauen stiftendes Kontrollgefühl auf Basis komplexer technischer Maßnahmen zu vermitteln. Vielmehr scheint es – zumindest im Einzelhandel – erforderlich, dem Kunden sehr einfach verständlich Schutzmaßnahmen anzubieten, wie etwa die Killfunktion oder eine Möglichkeit, den Tag abzureißen. Das im vorliegenden Bericht enthaltene Kapitel zu technischen Lösungsansätzen des UC geht auf die hier zur Verfügung stehenden Optionen in größerem Detail ein.

5.3.5 Wahrnehmung und Bewertung von individueller Ortung

Schließlich sei in diesem Zusammenhang noch auf eine weitere amerikanische Studie verwiesen, in der es darum geht zu differenzieren, in welchen Kontexten Menschen die Preisgabe persönlicher Informationen bzw. Beobachtung durch andere Parteien akzeptieren und in welchem Grad.[392] Dazu wurde 130 Versuchspersonen ein Szenario vorgestellt, in dem sie mit ihrem Handy geortet werden, wobei die Ortung mit der Weitergabe von Informationen zur Person verbunden ist. Sie wurden dazu befragt, wo sie persönliche Informationen mit unter-

[392] Lederer./ Mankoff et al.: Who Want to Know What When? Privacy Preference Determinants in Ubiquitous Computing, CHI 2003, Ft. Lauderdale, Florida, USA, ACM, 2003.

schiedlichem Auflösungsgrad zur Verfügung stellen würden. Es wurde zwischen engen Freunden/Partnern, Arbeitgebern, Fremden und kommerziell Werbetreibenden als Empfänger unterschieden, denen die Möglichkeit gegeben sein sollte, den Probanden beim geschäftlichen Mittagessen oder bei einer Abendveranstaltung zu orten. Die persönlichen Informationen über den Probanden beinhalteten entweder die wahre Identität mit Profilinformationen (E-Mail Adresse, Beruf, Interessen) und Angaben zur gegenwärtigen Aktivität (informationsintensive Ortung) oder eine pseudonyme Identität mit einer nur vagen Beschreibung der Aktivität und einer zweitrangigen E-Mail Adresse (informationsarme Ortung). Die Ergebnisse zeigen, dass es für eine Zustimmung zur Ortung und Informationspreisgabe wichtiger ist, *wer* die Ortung vornimmt als die Situation, in der die Ortung durchgeführt wird. Dieser Befund dreht sich nur um, wenn ein Arbeitgeber orten möchte. Hier spielt die Situation die bedeutendere Rolle. Handelt es sich um das Geschäftsessen zur Mittagszeit, darf der Arbeitgeber orten. Handelt es sich um die Abendveranstaltung, so wird einer informationsintensiven Ortung nicht zugestimmt oder eine Ortung grundsätzlich abgelehnt. Dies deutet darauf hin, dass die Akzeptanz von Überwachung grundsätzlich stark vom Vertrauen in den Informationsempfänger abhängt. Der Arbeitgeber jedoch nimmt eine Sonderrolle ein: Bei ihm wird die Legitimität der Ortung in der jeweiligen Situation in den Vordergrund gestellt.

5.4 Fokusgruppenerkenntnisse zum Thema Verbraucherängste bei der Einführung von RFID

1. Kontrollverlust über die eigenen Besitzgegenstände durch Unsichtbarkeit und Unbemerkbarkeit der RFID-Technik: Urangst, durch die Unsichtbarkeit und Unbemerkbarkeit der Technologie keine Kontrolle mehr darüber zu haben, was mit den eigenen Objekten passiert bzw. wann und ob diese ausgelesen werden:

- „... aber wenn man nicht weiß, wo dieses Ding ist? Und ich weiß nicht, ob es irgendwo draufklebt oder woanders drin ist?!
- „Das Produkt, das ich gekauft habe, ist in mein Eigentum übergegangen, und mit dem möchte ich machen können, was ich will. Das hat dann keinen mehr zu interessieren."

2. Verfolgbarkeit (engl. *Tracking*): Möglichkeit, dass Informationen über Objekte ausgelesen und für die Erstellung von Bewegungsprofilen genutzt werden könnten. Aufenthaltsorte von Individuen könnten über die Überwachung der ihnen zugehörigen Objekte auch über einen längeren Zeitraum hinweg zurückverfolgt werden.

- „Wenn sich diese Chip-Anwendung halt eben nur auf diesen Laden und den Anwender der Karte bezieht, ist das ja in Ordnung. Wenn aber eine Weiterverfolgung außerhalb des Ladens geschieht, hätte ich damit ein Problem."
- „Ich würde anfangen, unter Verfolgungsangst zu leiden…."

3. Informationssammlung und Personalisierung: Nutzung des EPCs als ID oder Merkmalsträger, um Personen auf Basis der ihnen zugehörigen Objekte wieder zu erkennen und einzuordnen. Eine Informationssammlung über die eigenen Einkäufe, Wiedererkennung und Einordnung, so wird befürchtet, könnten zu einer systematisch personalisierten Ansprache führen. Es wird ein potenziell diskriminierendes „Vorhalten eines Spiegels" be-

führen. Es wird ein potenziell diskriminierendes „Vorhalten eines Spiegels“ befürchtet.

- „…dann bringen sie mich in die niedrigere Preiskategorie und Frau Nachbarin steht daneben und sagt dann, guck´ mal, die kriegt nur so billige Sachen angeboten...“
- „Wenn jemand Informationen sammelt, und das bedeutet ja auch immer einen Zugriff auf eine Person, und man kennt diesen Zugriff nicht, man weiß nicht, dass da jemand zugreift, das ist ein unangenehmes Gefühl.“
- „Die wissen alles über mich, und ich weiß gar nichts über die.“

4. Objektverantwortlichkeit*:* Angst vor der Zuordnung von Personen zu den ihnen jetzt oder früher zugehörigen Objekten. Die Angst ist dadurch motiviert, dass man für den Missbrauch oder Verbleib von Objekten verantwortlich gemacht werden könnte. Dies mag vergleichsweise harmlose Beispiele betreffen, wie die weggeworfene Coladose im Wald, aber auch ernstere Fälle, wie lange verkaufte oder verschenkte Objekte, die in eine kriminelle Handlung involviert sind und den Verdacht auf den früheren Besitzer lenken.

- “ …sondern es geht mir darum, dass meine Persönlichkeit, meine Person selber nicht in Verbindung gebracht werden muss mit dem Produkt, nachdem ich es gekauft habe.“
- „Dann bin ich als Käufer für die Joghurtflasche verantwortlich oder was? Das ist doch bekloppt.“

5. Technologiepaternalismus: Möglichkeit, durch die der Technologie inhärente Objekt-Objekt-Erkennung kleinste Fehltritte systematisch und automatisch zu sanktionieren. So könnte die Papiertonne erkennen, dass fälschlicherweise eine Batterie in ihr landet, ein Medikamentenschrank, dass das Medikament vergessen wurde etc. Die resultierenden Warnsignale und Hinweise würden dem Menschen sein Fehlverhalten vorhalten, dieses womöglich öffentlich machen, sanktionieren oder automatisch unterbinden.

- “Die Frage ist doch, fängt es an zu piepsen, wenn ich einen Joghurt dann doch vor der Kasse abstelle, und dann gibt es ein Signal und dann wissen die aha …“
- „Dann stelle ich mir vor, ich nehme so irgendwie schönen Kaviar oder so und mein Computer sagt mir, das kriegst du nicht ...“

6. Krimineller Missbrauch: Befürchtung, dass Dritte (Nachbarn, Diebe, Hacker) die Technologie missbrauchen könnten, um den eigenen Besitz auszuspähen.

- „Ich finde es auch schrecklich und ich glaube auch, dass es ganz schnell für negative Situationen ausgenutzt werden kann.“
- „Ich glaube, dass es ganz schnell für negative Situationen ausgenutzt werden kann, für Spionage und alles mögliche.“

5.5 Risiken der „Embodied Virtuality“ und deren Wahrnehmung

Wie in Kap. 5.2.4 dargelegt, lässt sich neben Remote Access-Anwendungen im UC ein weiterer Servicetyp differenzieren: der der Embodied Virtuality. Hier geht es darum, dass Objekten eine „Intelligenz“ gegeben wird, die ihnen erlaubt, mit ihren Benutzern in eine unmittelba-

re Interaktion zu treten. Objekte sollen auf Menschen und Zustände reagieren und autonome bzw. teilautonome Entscheidungen treffen können. Die vier Szenarien der durchgeführten Studie sind Beispiele für diesen Typus von UC-Anwendungen: Der „intelligente Kühlschrank" beobachtet den Leerstand seines Inneren und schlägt auf Basis dieser Erkenntnis eine Einkaufsliste vor bzw. bestellt Fehlendes direkt beim Händler. Der „intelligente Arbeitsplatz" beobachtet die Haltung des Arbeitenden sowie seine Aktivitäten und passt die Einstellungen der Videokamera optimal auf den Nutzer an. Das „intelligente Auto" bemerkt, dass auf einer Strasse ein bestimmtes Tempolimit vorgeschrieben ist, gleicht dieses mit der Fahrgeschwindigkeit des Wagens ab und bremst automatisch bei Geschwindigkeitsüberschreitung. Ebenso untersucht es seinen Zustand im Hinblick auf Wartungsnotwendigkeiten und bestellt einen Termin bei der Werkstatt, falls eine Reparatur fällig ist. In all diesen Szenarien reagiert das Objekt auf einen Zustand oder auf den Menschen direkt und tritt mit dem Menschen in Interaktion.

Bei solchen Interaktionen zwischen Menschen und ihren Objekten fallen selbstverständlich Daten an, die in verdichteter Form ebenso ein Überwachungsproblem hervorrufen können wie Remote Access-Anwendungen. Wenn der Kühlschrank beispielsweise seine Bestände ausliest und diese Information an den Handel weiterleitet, könnte ein Datenschutzproblem entstehen. Ebenso könnte der eingangs erwähnte Spiegel den Eltern mitteilen, ob ihr Kind die Zähne schon geputzt hat und wie lange. Jedoch könnte es sich in vielen Fällen technisch auch um lokal abgrenzbare Applikationen handeln, welche nur solche Daten verarbeiten, die für die unmittelbare Interaktion absolut notwendig sind und keine Schnittstellen zu weitergehenden Informationsdiensten beinhalten. Ebenso sind anonyme und pseudonyme Gestaltungsmöglichkeiten denkbar, etwa durch Einbeziehung einer vertrauenswürdigen dritten Partei (zu Englisch „trusted third party").

Aus Sicht des Nutzers entstehen bei der Interaktion mit intelligenten Objekten jedoch auch völlig andere Probleme als der Erhalt von Privatsphäre, nämlich die der *physischen* Kontrolle über dieselben (im Gegensatz zur informationellen Kontrolle). Wie die Fokusgruppen mit Verbrauchern ergeben haben (siehe Kap. 5.4) besteht ein potenzielles Problem im Umgang mit Objekten, welches man auch als „Technologiepaternalismus" bezeichnen könnte. Technologiepaternalismus beinhaltet kurz gesprochen, dass die Maschine bzw. das Objekt automatisch Fehlverhalten sanktioniert oder dieses gar nicht erst zulässt. Ein Beispiel ist das Warnsignal im Auto, welches ertönt, wenn der Fahrer sich nicht anschnallt. Der Wagen hat das letzte Wort, denn der Fahrer muss sich anschnallen, wenn er dem Signalgeräusch entkommen möchte. Er hat keine Kontrolle über den Vorgang.

Technologiepaternalismus wurde an anderer Stelle wie folgt definiert:[393]

Angenommen eine Technologie (T) ist kontrolliert (oder gebaut) von einem „Pater" (P) und führt eine Aktivität (A) aus, die ein Individuum (I) direkt betrifft, dann ist T paternalistisch unter der Bedingung, dass

[393] Spiekermann / Pallas: Technology Paternalism - Wider Implications of RFID and Sensor Networks, Poiesis & Praxis - International Journal of Ethics of Science and Technology Assessment 4, 2005.

- Aktivität A vom Individuum I als limitierend, strafend oder in einer anderen Form freiheitsbeschränkend empfunden wird UND
- das Individuum I A nicht vermeiden oder überstimmen kann, ohne dabei Funktionalität von T einzubüßen, UND
- A vom Pater P so dargestellt wird, dass A hauptsächlich im Interesse des Individuums existiert, UND
- A autonom durchgeführt wird.

Technologiepaternalismus ist sicherlich eine extreme Form von Autonomie in Systemen, die bei Nutzern auf eine geringe Akzeptanz stoßen dürfte, wenn diese in der Tat anders handeln möchten, als das System es vorschreibt (siehe Fokusgruppenergebnisse in Kap. 5.4). Die Fragen, die sich hier stellen, sind gesellschaftspolitischer Natur: Dürfen technische Systeme den Handlungsspielraum von Menschen begrenzen und wenn ja, unter welchen Umständen? Sollten rechtliche Grenzen durch Technik „in Beton" gegossen werden dürfen? Oder sollten Menschen trotz rechtlichen Rahmens immer noch ein letztes Wort haben dürfen? Sollte es Produktherstellern erlaubt sein, mittels RFID-Technik Produkte zu bündeln und ihr Funktionieren vom Vorhandensein komplementärer Komponenten abhängig zu machen?[394] Wie autonom dürfen Objekte handeln? Und wer haftet, wenn Systeme Fehler machen und Menschen zu falschen Handlungen zwingen (zum Beispiel Fahrblockade des Alcokey im Notfall)?

Auch bei der Beantwortung dieser Fragen können ökonomische, soziale und politische Motive eine Rolle spielen. Man nehme zum Beispiel den von Saab vorgestellten Alcokey. In diesen muss der Fahrer pusten, um zu beweisen, dass er keinen Alkohol im Blut hat. Stellt der Schlüssel mittels Sensoren fest, dass der Fahrer nicht fahrtauglich ist, so erlaubt er nicht mehr, den Wagen anspringen zu lassen.

Sicherlich hätten einige Eltern Interesse daran, ihren Kindern solche Wagenschlüssel mit auf die Reise zu geben (soziales Motiv). Ebenso wären Kfz-Versicherungen für solche Geräte, da man davon ausgehen kann, dass die Alkohol bedingte Unfallrate entfallen würde (ökonomisches Motiv). Auch der Staat würde den Einsatz solcher Systeme sicherlich gutheißen, da die Einhaltung des Fahrverbots bei Alkohol endlich gesichert wäre (politisches Motiv). Trotzdem stellt sich die Frage, inwieweit Menschen nicht weiterhin in der Lage bleiben sollten, Entscheidungen dieser Art selbst zu treffen. Möglicherweise verträgt die Gesellschaft nur einen gewissen Grad an Konformität? Und braucht auch einen gewissen Grad an Freiheit, um Entscheidungsfähigkeit beizubehalten?

Im Rahmen der Studie wurde untersucht, inwieweit die Kontrolle in Form „des letzten Wortes" des Menschen im Umgang mit Technik für die UC-Technologien eine Rolle spielt.

[394] Eine derartige Bündelung von Produkten wird heute schon an vielen Stellen praktiziert, z.B. bei Druckern, für die herstellerspezifische Druckerpatronen bezogen werden müssen. RFID könnte diese Art von Produktbündelung jedoch deutlich ubiquitärer machen, als dies heute der Fall ist.

5.6 Empirische Erkenntnisse zur Bedeutung von Kontrolle im Umgang mit intelligenten Objekten

Im Rahmen der vorliegenden Studie war die Variation von Kontrolle über den dargestellten UC-Dienst ein wesentlicher Untersuchungsbestandteil. Abbildungen 17 bis 20 zeigen, wie die Kontrolle über die UC-Dienste in der Befragung variiert wurden. Jeweils 50 % der Teilnehmer sahen die vier Szenarien entweder in einer Version mit hoher Kontrolle (sie hatten das letzte Wort) oder in einer Version mit niedriger Kontrolle (die Technik hatte das letzte Wort). Die Zuteilung zu der einen oder anderen Version erfolgte zufällig. Die Kontrollmanipulation war anhand des 10-Stufenmodells zur Kontrollvariation von Sheridan[395] aufgebaut, der unterschiedliche Grade der Kontrolle für elektronische Assistenzsysteme unterscheidet. Die hohe Kontrolle entsprach in den Szenarien jeweils der dritten Stufe dieses Modells, welche besagt:

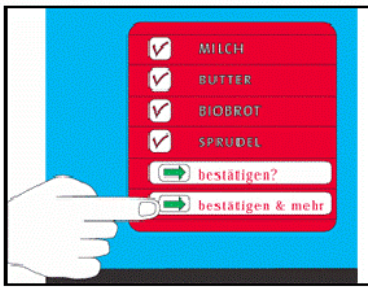
- Der Computer listet nicht nur alle Handlungsoptionen auf, sondern schlägt auch eine davon dem Operateur zur Ausführung vor, der sie jedoch nicht befolgen muss.

Die niedrige Kontrolle entsprach jeweils der siebten Stufe des Sheridan-Modells, welche besagt:

- Der Computer erledigt die gesamte Aufgabe und informiert selbständig und vollständig den Operateur über die gewählte Aktion und ihre Ausführung.

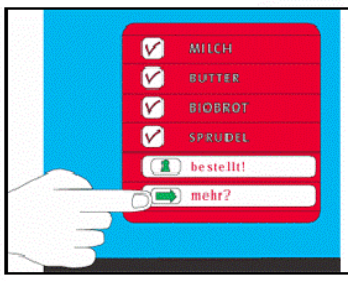
Variation im Szenario „Intelligenter Kühlschrank“

Hohe Kontrolle



Text a): „…Was fehlt, wird mir auf dem EZ-Bildschirm am Kühlschrank angezeigt und ich kann die entsprechenden Produkte zum Nachkauf bestätigen.“

Niedrige Kontrolle

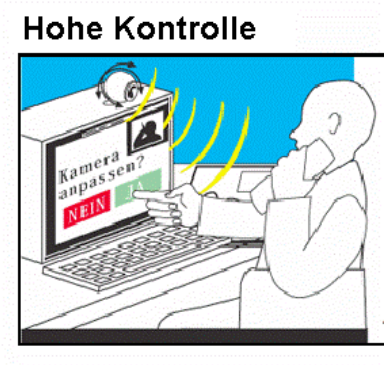


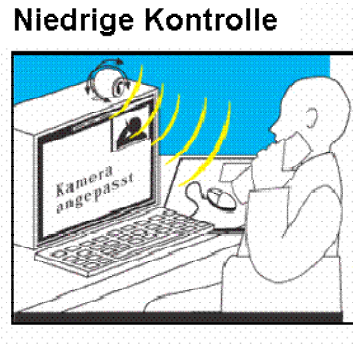
Text b): „…Ist nicht mehr genug da, wird der Bedarf von ihm automatisch ermittelt und sofort nachbestellt. Auf dem EZ-Bildschirm am Kühlschrank wird mir die Liste mit den bestellten Produkten angezeigt.“

Abbildung 22: Szenariovariation Kühlschrank

[395] Sheridan: Task allocation and supervisor control, Handbook of Human-Computer Interaction, M. Helander, Amsterdam, North-Holland: Elsevier Science Publisher, 1988, S. 159-173.

Variation im Szenario „Intelligenter Arbeitsplatz“





Text a): „…Wenn ich zum Beispiel telefoniere, bietet er an, die Kamera des Bildtelefons einzuschalten und optimal auf mich einzuschwenken.“

Text b): „…Wenn ich zum Beispiel telefoniere, schaltet er automatisch die Kamera des Bildtelefons ein und schwenkt diese optimal auf mich“

Abbildung 23: Szenariovariation Arbeitsplatz

Variation im Szenario „Automatische Bremse“

Text a): „…Das Navigationssystem schlägt mir vor, dass ich den Wagen aufgrund der Geschwindigkeitsbegrenzung abbremsen sollte.“

Text b): „…Das Navigationssystem informiert mich, dass es den Wagen aufgrund der Geschwindigkeitsbegrenzung abgebremst hat.“

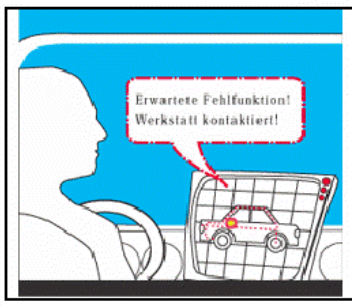
Abbildung 24: Szenario Fahrzeug mit automatischer Bremse

Variation im Szenario „Automatische Selbstwartung“

Hohe Kontrolle

Text a): „….Stellt das Auto fest, dass ein Teil demnächst kaputt gehen wird, weil offizielle Schadenswerte über- oder unterschritten sind, so schlägt es vor, selbständig die Werkstatt zu kontaktieren und die Bestellung des entsprechenden Ersatzteils zu veranlassen.“

Niedrige Kontrolle



Text b): „…Stellt das Auto fest, dass ein Teil demnächst kaputt gehen wird, weil offizielle Schadenswerte über- oder unterschritten sind, so kontaktiert es selbständig die Werkstatt und veranlasst die Bestellung des entsprechenden Ersatzteils.“

Abbildung 25: Szenario Fahrzeug mit automatischer Selbstwartung

Für jedes Szenario wurde bei jeder Gruppe abgefragt, inwiefern ein Kontrollbedürfnis besteht (Abbildung 25).[396] Dabei zeigt sich, dass dieses insbesondere bei den Heimanwendungen Kühlschrank und Arbeitsplatz deutlich höher ist als bei den Szenarien, welche sich auf das Auto und somit auf die Straße beziehen. Dies könnte ein Hinweis darauf sein, dass Kontrolle, insbesondere in den eigenen vier Wänden, besonders wichtig ist oder dass die Straße und die Nutzung von Fahrzeugen ohnehin (und aus gutem Grund) schon so reguliert sind, dass Menschen hier eine geringere Kontrollerwartung haben. Eine geringe jedoch signifikante Korrelation zwischen dem Kontrollbedürfnis und dem Risiko, ohne das System Fehler zu machen, lässt die Hypothese zu, dass ein Kontrollbedürfnis dann geringer ist, wenn man durch das System das Risiko reduzieren kann, Fehler zu machen.

Dem Kontrollbedürfnis wurde die Messung der tatsächlich wahrgenommenen Kontrolle gegenübergestellt.[397] Aus diesen beiden Konstrukten wurde eine Kontrollbilanz ermittelt, die sich als Differenz zwischen Kontrollbedürfnis und tatsächlich wahrgenommener Kontrolle ergibt. Abbildung 27 zeigt, dass erwartungsgemäß diejenigen Teilnehmer, welche in der „Low Control“-Gruppe waren auch eine durchgängig signifikant negativere Kontrollbilanz

[396] Zur Messung des Kontrollbedürfnis wurden zwei Fragen gestellt: Erstens, ob man jederzeit bestimmen möchte, was geschieht (z.B. „Ich möchte jederzeit bestimmen, was eingekauft wird.“). Und zweitens, ob es einem besonders wichtig ist, selbst zu bestimmen, was geschieht (z.B. „Selbst zu bestimmen, was eingekauft wird, ist mir besonders wichtig.“). Die beiden Items waren im Ergebnis für alle Szenarien hoch korreliert.

[397] Hier wurde gefragt, ob die Teilnehmer das Gefühl haben, dass es ihnen mit dem System möglich ist, jederzeit selbst über die Tätigkeit zu bestimmen, und ob das System ihnen ausreichend Kontrolle lässt.

aufweisen als diejenigen, denen immer noch das letzte Wort blieb. Trotzdem ist zu konstatieren, dass unabhängig von der Kontrollgruppe alle Szenarien in der Befragung bei den Teilnehmern zu einer negativen Kontrollbilanz führen. Das heißt, dass alle Teilnehmer durchgängig weniger Kontrolle empfunden haben als ihnen lieb ist.

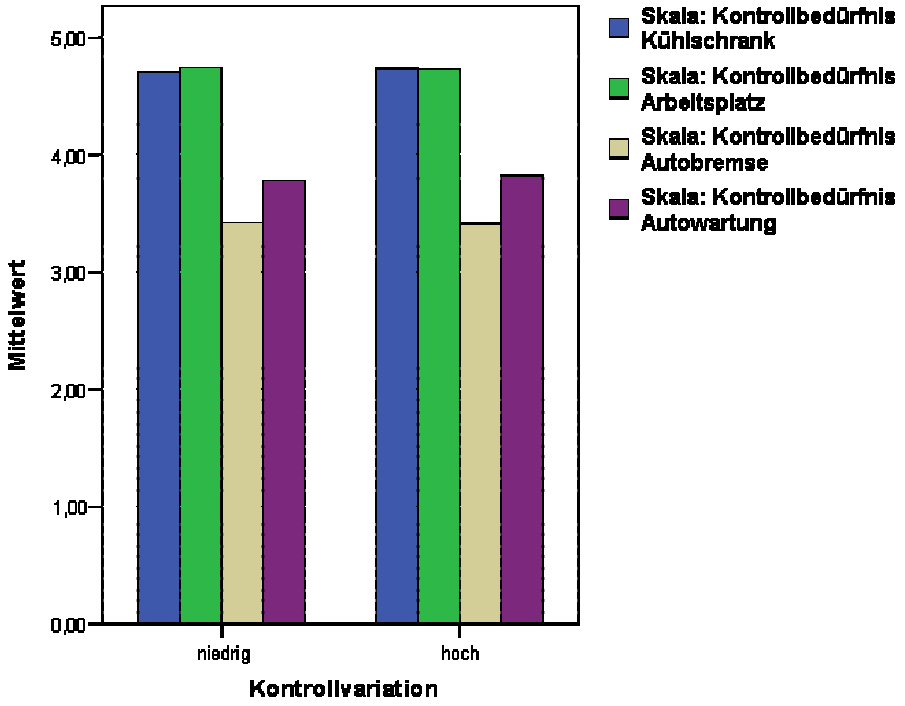


Abbildung 26: Kontrollbedürfnis in den beiden Kontrollgruppen

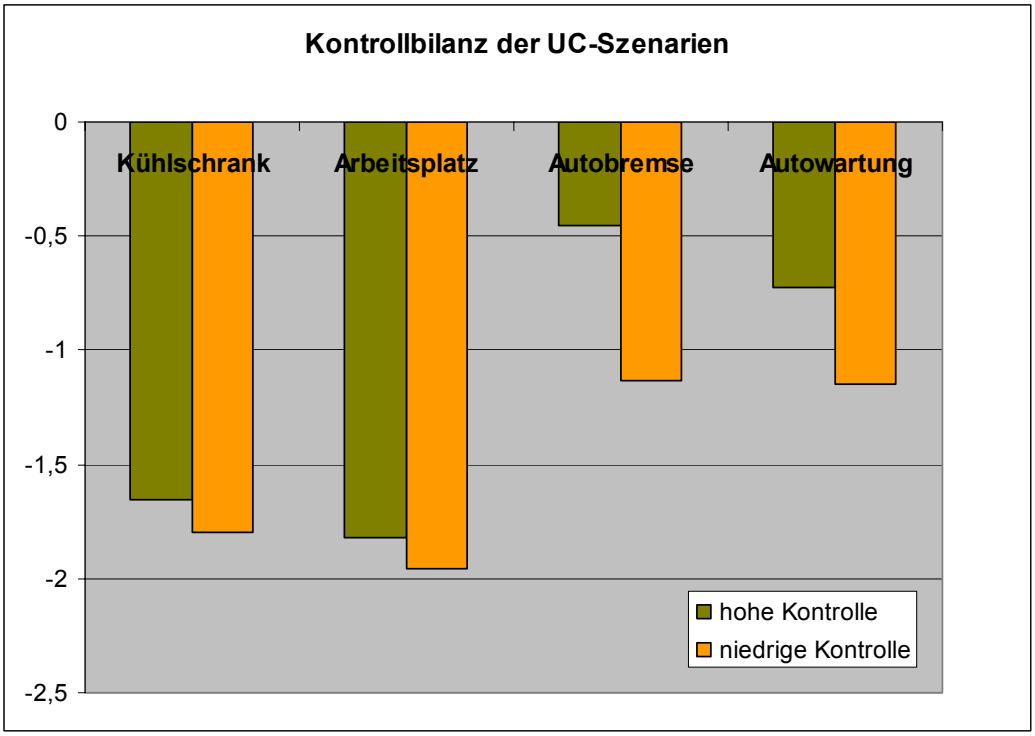


Abbildung 27: Kontrollbilanzen

Entscheidend ist in einem nächsten Schritt zu untersuchen, welche Folgen die wahrgenommene Kontrolle für die Beurteilung eines UC-Szenarios hat. Wie oben bereits angedeutet, legen unsere Daten nahe, dass die Kontrollwahrnehmung (Kontrollbilanz) einen großen Einfluss auf die Akzeptanz von UC-Services hat. Abbildung 28 zeigt die gemessenen Einflüsse noch einmal in größerem Detail („o“ steht für Online, „p“ für Papier).

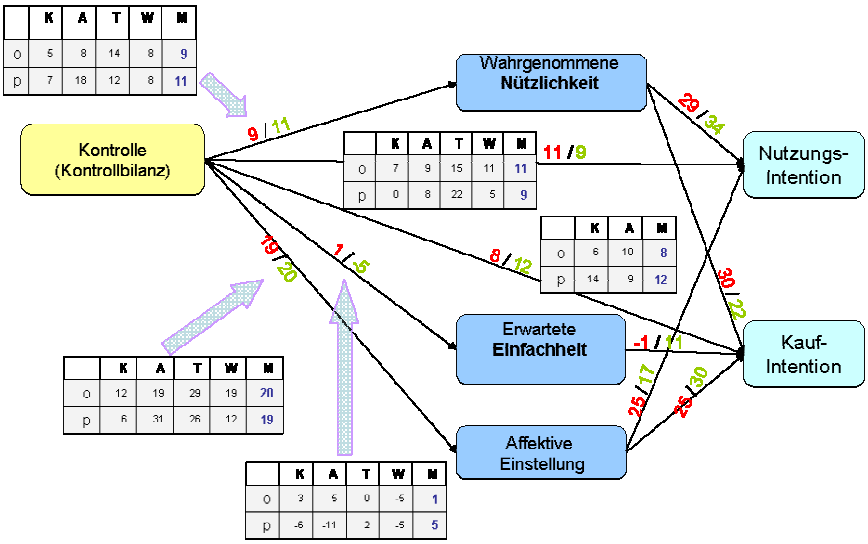


Abbildung 28:

Einfluss der Kontrolle auf die Akzeptanz; Ergebnisse einer Regressionsanalyse (beide Stichproben zusammen)

Hier zeigt sich, dass Kontrolle den größten direkten Einfluss auf die affektive Reaktion ausübt und über diese dann auf die Kauf- und Nutzungsintention wirkt. Ebenso beeinflusst Kontrolle die wahrgenommene Nützlichkeit sowie direkt die Kauf- und Nutzungsintention. Am wichtigsten ist die Kontrolle bei der Ausübung der Bremsfunktion im Auto. Allerdings beurteilen die auf Papier Befragten den Einfluss von Kontrolle an einigen Stellen anders als die online Befragten. Für die auf Papier Befragten nimmt nämlich Kontrolle über den automatisch agierenden Arbeitsplatz ein fast genauso großes (zum Teil größeres) Gewicht ein als Kontrolle über das Auto. Dies ist bei den online Befragten nicht so. Dieses Ergebnis legt nahe, dass die Kontrollwahrnehmung sehr stark von der individuellen Anwendung geprägt ist und möglicherweise von der Erfahrung und dem Kontext, den der Einzelne mit dem Bereich verbindet, in dem UC-Technik eingesetzt werden soll.

Eine Gegenüberstellung der Kontrollvariationen (Appendix 8) legt darüber hinaus nahe, dass eine hohe Kontrolle, wo der Verbraucher das letzte Wort hat, Vertrauen in den Service ansteigen lässt. Ebenso führt mehr Kontrolle zu einer Reduzierung der mit den Szenarien verbundenen Risikowahrnehmung. Je mehr Kontrolle, desto geringer das erwartete Risiko, dass ein System nicht in den eigenen Alltag passen könnte. Je mehr Kontrolle, desto geringer das erwartete Risiko, dass das System die Privatsphäre beeinträchtigen könnte. Und je mehr Kontrolle, desto geringer auch das erwartete Risiko, dass das System zu Zeitverlusten führen könnte (Appendix 8)

Insgesamt zeigen die Ergebnisse, dass es für die Anbieter von UC-Services von großer Bedeutung ist, die letztendliche Kontrolle über die Systeme beim Nutzer zu belassen. Auch politisch sollte hinterfragt werden, inwieweit die Nutzerkontrolle nicht eine generelle Richtlinie für Hersteller werden sollte.

5.7 Zusammenfassung und Schlussfolgerungen

Informations-, Kommunikations- und Automatisierungsdienste, die mittels UC-Technologie immer häufiger zum Einsatz kommen sollen, werden von Verbrauchern relativ positiv bewertet. Insbesondere solche Dienstleistungen, die zu Zeitersparnis führen oder dabei helfen, bisher vorhandene Produktrisiken zu reduzieren, werden geschätzt. Allerdings scheint diese positive Beurteilung in einem Spannungsverhältnis mit einem potenziellen Kontrollverlust zu stehen. Dieser Kontrollverlust kann zum einen in einer Aufgabe der informationellen Selbstbestimmung liegen; z.B. wenn RFID-Lesegeräte unbemerkt auf Chips in den eigenen Gegenständen zugreifen. Zum anderen kann auch das autonome Handeln von intelligenten Objekten zu einem physischen Kontrollverlust führen. Die Wahrnehmung beider Arten von Kontrollverlust führt bei den untersuchten Verbrauchern zu einer Reduzierung der Kauf- und Nutzungsintention von UC-Dienstleistungen.

Es ist daher aus ökonomischer Sicht sinnvoll, Verbraucherbedenken proaktiv zu begegnen, indem bewusst eine Kontrolle über UC-Dienstleistungen gewährleistet wird. Diese sollte objektiv wirksam und leicht vermittelbar sein, denn komplexen Privacy Enhancing Technologies wird – so legen es einige Untersuchungen nahe – wenig vertraut (evtl. auch aufgrund von Unverständnis).

Die Untersuchungen zur Wahrnehmung von Datenverarbeitung und Datenschutz legen nahe, dass ein nicht unbedeutender Teil der deutschen Verbraucher sehr wenig Verständnis dafür hat, was Datenverarbeitung bedeutet. Die Mehrheit scheint zwar um die Existenz einer kommerziellen Datenverarbeitung zu wissen. Konsequenzen derselben für jeden Einzelnen scheinen den meisten jedoch wenig transparent. Insgesamt wird an ein hohes Schutzniveau durch Gesetze geglaubt. Eine diskriminierende Nutzung von Informationen wird von der Mehrheit weder erwartet noch gewünscht.

5.8 Literatur

Acquisti, Alessandro / Grossklags, Jens: Privacy and Rationality in Individual Decision Making, IEEE Security & Privacy. 2, 2005, S. 24-30.

Adams, Anne / Sasse, Angela: Taming the Wolf in Sheep's Clothing: Privacy in Multimedia Communications. Multimedia99, Orlando, Florida, USA, 1999.

Alahuhta, Petteri / De Hert, Paul / et al.: Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities, Safeguards in a World of Ambient Intelligence (SWAMI), Editors: Punie, Delaitre, Maghiros and Wright, Brussels, 2005.

Altman, Irwin: The environment and social behavior: Privacy, personal space, territory, crowding. Monterey, California, Brooks/Cole, 1975.

Berendt, Bettina / Guenther, Oliver / et al.: Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, Communications of the ACM 48(4), 2005.

Berthold, Oliver / Guenther, Oliver / et al.: RFID Verbraucherängste und Verbraucherschutz." Wirtschaftsinformatik Heft 6, 2005.

Beslay, Laurent / Hakala, Hannu (forthcoming in 2005): Digital Territory: Bubbles.

Boyle, Michael: A Shared Vocabulary for Privacy, Fifth International Conference on Ubiquitous Computing, Seattle, Washington, 2003.

Cox, Donald F.: Synthesis: Risk taking and information handling in consumer behavior, Boston, MA, Harvard University Press, S. 604-639.

Cox, Jennifer: Can differential prices be fair?, The Journal of Product and Brand Management 10(4), 2001, S. 264-276.

Cunningham, Scott M.: The Major Dimensions of Perceived Risk, Risk Taking and Information Handling in Consumer Behavior, D. Cox. Cambridge, MA, Harvard University Press, 1967.

Davis, Fred: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology., MIS Quarterly 13(3), 1989, 319-340.

Davis, Fred / Bagozzi, Richard / et al.: User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, Management Science 35(8), 1989, S. 982-1003.

Duce, Helen: Public Policy: Understanding Public Opinion. A.-I. Center, Cambridge, UK, University of Cambridge, UK, 2003.

Groebel, Jo / Koenen, Andrea / et al.: Deutschland und die digitale Welt. Internet 2002: Deutschland und die digitale Welt. Internetnutzung und Medieneinschätzung in Deutschland und Nordrhein-Westfalen im internationalen Vergleich, Groebel Jo / Gehrke, Gernot: Opladen, Schriftenreihe Medienforschung der LfM, 46, 2002.

Guenther, Oliver / Spiekermann, Sarah: RFID and Perceived Control - The Consumer's View, Communications of the ACM 48(9), 2005, S. 73-76.

Hilty, Lorenz: Electronic waste - an emerging risk?" Environmental Impact Assessment Review 25, 2005, S. 431– 435.

Kang, Jerry / Cuff, Dana: Pervasive Computing: Embedding the Public Sphere, Public Law & Legal Theory Research Paper Series, Los Angeles, US, University of California, Los Angeles School of Law, 62, 2005.

Lahlou, Saadi / Langheinrich, Marc / et al.: Privacy and trust issues with invisible computers, Communications of the ACM 48(3), 2005, S. 59-60.

Lederer, Scott / Mankoff, Jennifer / et al.: Who Want to Know What When? Privacy Preference Determinants in Ubiquitous Computing, CHI 2003, Ft. Lauderdale, Florida, USA, ACM, 2003.

McCahill, Michael / Norris, Clive.: CCTV in London, C. f. C. a. C. Justice. Hull, UK, 2002.

Microsoft: Smarter Retailing: Innovation at the Edge of the Retail Enterprise, Microsoft, 2004.

Myles, Ginger / Friday, Adrian / et al.: Preserving Privacy in Environments with Location-Based Applications, IEEE Pervasive Computing. 2, 2003, S 56 - 64.

Parasuraman, Raja / Riley, Victor: Humans and Automation: Use, Misuse, Disuse, Abuse, Human Factors and Ergonomics Society 39(2), 1997, S. 230-253.

Roussos, George / Moussouri, Theano: Consumer perceptions of privacy, security and trust in ubiquitous commerce, Personal and Ubiquitous Computing 8, 2004, S. 416-429.

Sheridan, Thomas B.: Task allocation and supervisor control, Handbook of Human-Computer Interaction, M. Helander. Amsterdam, North-Holland: Elsevier Science Publisher, 2004, S. 159-173.

Solove, Daniel J.: A Taxonomy of Privacy, University of Pennsylvania Law Review 154, 2005.

Spiekermann, Sarah: Individual Price Discrimination - An Impossibility, Berlin, Institute of Information Systems, Humboldt University Berlin, 2005.

Spiekermann, Sarah / Pallas, Frank: Technology Paternalism - Wider Implications of RFID and Sensor Networks, Poiesis & Praxis - International Journal of Ethics of Science and Technology Assessment 4, 2005.

Spiekermann, Spiekermann / Rothensee, Matthias: Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing, I. f. Wirtschaftsinformatik, Berlin, Humboldt-Universität zu Berlin, 2005.

Venkatesh, Viswanath / Davis, Fred: A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies, Management Science 46(2), 2000, S. 186-204.

Walker, Guy H. / Stanton, Neville / et al.: Where is Computing in Driving Cars?, International Journal of Human-Computer Interaction 13(2), 2001, S. 203-229.

Weiser, Mark: The Computer for the 21st Century, Scientific American, 265, 1991, S. 94-104.

Weiser, Mark / Brown, John Seely: The Coming Age of Calm Technology, Xerox Parc, 1996.

Welzel, Peter / Filipova, Lilia: Reducing Asymmetric Information in Insurance Markets: Cars with Black Boxes, Volkswirtschaftliche Diskussionsreihe, U. A. Institut für Volkswirtschaftslehre. Augsburg, 2005.

6 Datenschutzrechtliche Risiken des Ubiquitous Computing und rechtliche Möglichkeiten des Risikomanagements

Jan Möller, Johann Bizer

6.1 Einleitung

Vielfältige rechtliche Rahmenbedingungen beeinflussen als Faktoren die technische Entwicklung, die gesellschaftliche Akzeptanz und damit nicht zuletzt den wirtschaftlichen Erfolg von Anwendungen des Ubiquitous Computing. Diese Bestimmungsfaktoren werden im Kapitel 3 (Recht) dieser Studie beschrieben und in bestehende oder wahrscheinliche Anwendungszusammenhänge gestellt. Der Einsatz allgegenwärtiger Datenverarbeitungstechniken in Anwendungen des täglichen Lebens wird Folgen für die Menschen, aber auch für die Gesellschaft als Ganzes haben. Eine entscheidende Rolle kommt hierbei dem Überwachungspotential der Anwendungen des Ubiquitous Computing zu[398] und wie die Betroffenen mit diesem Potential umgehen werden.

Das Wissen über die Lebensumstände, Handlungsweisen und Vorlieben von Menschen gewinnt für die Ausrichtung von Geschäftsmodellen eine immer größere Bedeutung. Techniken der Datenverarbeitung wie das Data Mining ermöglichen eine übergreifende Auswertung personenbezogener Daten. Kundendaten können mit anderen Informationen über Verhalten und Vorlieben sowie soziodemographischen Informationen zusammengeführt werden, um ein auf Kundentypen, aber auch individuelle Kunden ausgerichtetes Marketing zu ermöglichen.[399] Gleichzeitig ist zu beobachten, dass staatliche Stellen sukzessive ihre Erhebungsbefugnisse ausweiten, indem sie Zugriff auf die von Unternehmen gewonnenen Kundendaten nehmen.[400] Gleichzeitig birgt ein (intransparenter) Informationsvorsprung einer Partei, unabhängig davon, ob es sich um eine private oder öffentliche Stelle handelt, ein erhebliches Potential, um das Gleichgewicht zwischen Vertragsparteien und Kommunikationspartnern durch eine Machtverschiebung zu stören, die von der informierten Partei zum eigenen Vorteil genutzt werden kann.

Wie auch immer sich die Folgen für den Betroffenen darstellen, die Entscheidung darüber, ob und wie einmal erhobene oder erzeugte und Dritten bekannt gewordene Informationen genutzt werden, entzieht sich weitgehend der Kontrolle des Betroffenen. Welche Sensoren

---

[398] Vgl. z.B. Weichert: Die Fußball-WM als Überwachungs-Großprojekt, DANA 01/2005, S. 7 (8); Holznagel / Bonnekoh: Radio Frequency Identification – Innovation vs. Datenschutz?,. MMR 2006, S. 17 (21).

[399] Jacob / Jost, Marketingnutzung von Kundendaten und Datenschutz, DuD 2003, 621 ff.; Petri / Kieper, Datenbevorratungs- und -analysesysteme in der Privatwirtschaft, DuD 2003, 601 ff.

[400] Ein Bespiel ist der staatliche Zugriff auf Kontoinformationen bei den Kreditinstituten nach § 93 Abs. 7, 8 und 93 b AO sowie § 24 c KWG. Ein anderes Beispiel ist der Online-Zugriff auf die Kundendaten der TK-Unternehmen nach § 112 TKG.

bzw. Lesegeräte die Signale der Objekte, die der Betroffene mehr oder weniger zufällig mit sich führt oder trägt, unbemerkt auslesen und durch Hintergrundsysteme verarbeiten und wer für diese Verarbeitung ihm gegenüber verantwortlich ist, entzieht sich seiner Kenntnis. Solchen technikbedingten Kontrollverlusten wird man zumindest durch gesonderte organisatorische Maßnahmen auf unterschiedlichen Ebenen begegnen müssen.

Auf staatlicher Ebene kann das Recht eine ordnende Funktion übernehmen und Machtverschiebungen durch einen einseitigen Informationsvorsprung verhindern oder ausgleichen. Beispielhaft für einen derartigen Machtausgleich ist das Verbraucherschutzrecht.[401] Ausgleichseffekte gegen ein einseitig übervorteilendes Handeln können aber auch durch Regelungen in anderen Rechtsgebieten erreicht werden. So kann für das Umfeld allgegenwärtiger Datenverarbeitung neben datenschutzrechtlichen Vorgaben auch ein angemessen ausgestaltetes Haftungsrecht von Bedeutung sein, um die Verantwortung der Anwender gegenüber den von einer Erfassung Betroffenen zu stärken.[402]

Die Wirksamkeit derartiger rechtlicher Regelungen setzt allerdings die Möglichkeit des Rechteinhabers voraus, dieses auch durchzusetzen. Die allgegenwärtige Datenverarbeitung wird aufgrund ihrer technischen und strukturellen Eigenschaften das bestehende Rechtsschutzsystem vor erhebliche Herausforderungen stellen, denn die Betroffenen müssen erst einmal in Erfahrung bringen können, dass ihre Daten ausgelesen worden sind. Wirksame Maßnahmen sind daher nicht allein im rechtlichen oder technischen Umfeld zu suchen, sondern werden nur in einem abgestimmten Zusammenspiel von rechtlichen und technischen Maßnahmen erfolgreich sein. Ökonomische Sekundäreffekte bewusster Technik- und Rechtsgestaltung sollten dabei gezielt einbezogen und zur sozialadäquaten Steuerung des Einsatzes von Anwendungen allgegenwärtiger Datenverarbeitung im Alltag eingesetzt werden.

Dieses Kapitel arbeitet unter rechtlichen Gesichtspunkten die Risiken exemplarischer Anwendungen des Ubiquitous Computing für das informationelle Selbstbestimmungsrecht heraus. Die Darstellung orientiert sich an Beispielen, weil viele UC-Anwendungen noch in der Entwicklung oder am Übergang in eine massenhafte Verbreitung stehen. Die Frage, ob und wie sich ein Risiko realisieren wird, hängt im Wesentlichen von der Art ihrer Implementierung und ihrem konkreten Einsatzumfeld ab. Bei der Beschreibung der Risiken wird auf das im Kapitel 1 beschriebene generische Modell einer UC-Anwendung zurückgegriffen.

Das Bundesverfassungsgericht hat dem Gesetzgeber aufgegeben „wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels, […] die technischen Entwicklungen aufmerksam zu beobachten und notfalls durch ergänzende Rechtssetzung korrigierend einzugreifen.“[403] Damit der Gesetzgeber dieser Aufgabe nachkommen kann, stellen wir Maßnahmen vor, um diesen Risiken durch rechtliche Regelungen bzw. als rechtliche Rahmenbedingungen technischer Schutzmaßnahmen entgegenwirken zu können.

---

[401] Borchert, Verbraucherschutzrecht, S. 1.

[402] Ausführungen zu den „Verantwortungsräumen“ s.u. Kap. 6.3.2, zur „Nutzerzentrierten Gefährdungshaftung“,. s.u. Kap. 6.3.6.2.

[403] BVerfG 2 BvR 581/01, MMR 2005, S. 371.

Das Kapitel schließt mit einer Zusammenfassung der Ergebnisse.

6.2 Risiken des Ubiquitous Computing für die informationelle Selbstbestimmung

Zentrale Risiken für die informationelle Selbstbestimmung ergeben sich einerseits aus den Grundstrukturen der allgegenwärtigen Datenverarbeitung, andererseits aus Problemen einzelner funktionaler Bestandteile des Ubiquitous Computing.

6.2.1 Strukturelle Risiken

Strukturelle Risiken ergeben sich - getrieben durch die Globalisierung - aus der Internationalisierung der Datenverarbeitung (s.u. Kap. 6.2.1.1), der Tendenz zur Diversifizierung und damit zum Outsourcing der Datenverarbeitung (s.u. Kap. 6.2.1.2), den damit verbundenen Problemen für die Durchsetzung des Datenschutzes (s.u. Kap. 6.2.1.3) sowie der technisch möglichen Bildung von Bewegungsprofilen der Nutzer (s.u. Kap.6.2.1.4).

6.2.1.1 Internationalität von personenbezogenen Datenverarbeitungen

UC-Systeme sind grundsätzlich netzbasiert ausgelegt, so dass personenbezogene Daten an unterschiedlichen Orten und damit, soweit bspw. das Internet genutzt wird, auch international verarbeitet werden können. Dies wirft in jedem Einzelfall die Frage auf, welches Datenschutzrecht Anwendung finden wird.

Grundlage des deutschen wie des europäischen Datenschutzrechts ist das Sitzlandprinzip. Maßgebend ist also nicht der Ort der Verarbeitung, sondern der Sitz der für die Verarbeitung personenbezogener Daten verantwortlichen Stelle.[404] Alle datenschutzrelevanten Erhebungen, Verarbeitungen und Nutzungen personenbezogener Daten in UC-Systemen unterliegen, soweit sie von verantwortlichen Stellen mit Geschäfts- oder Wohnsitz in Deutschland oder auf Servern in Deutschland durchgeführt und nicht nur durchgeleitet werden, den Anforderungen des deutschen Datenschutzrechts.[405] Werden personenbezogene Daten von einem Nutzer in Deutschland von einer verantwortlichen Stelle erhoben, die ihren Sitz in der Europäischen Union oder einem Staat des Europäischen Wirtschaftsraums (EWR) hat, dann ist das nationale Datenschutzrecht des Mitgliedstaates anzuwenden, in dem die verantwortliche Stelle ihren Sitz hat. Ein einheitliches Datenschutzniveau ist nach der Konstruktion des Europäischen Datenschutzrechts dadurch gewährleistet, dass die Mitgliedstaaten ihr nationales Datenschutzrecht an den Mindestanforderungen der europäischen Datenschutzrichtlinie ausrichten müssen.[406] Eine innerhalb des Geltungsbereichs der EU-Datenschutzrichtlinie verteilte Verarbeitung personenbezogener Daten im Rahmen einer UC-Anwendung hätte mit

[404] Dammann / Simitis, Art. 4 Anmk. 2; Dammann in: Simitis, BDSG, § 1, Rn. 197 ff.

[405] Vgl. § 1 Abs. 5 Satz 1, § 4 b und § 4 c BDSG.

[406] EG-Datenschutz-Richtlinien 95/46/EG sowie 2002/58/EG.

anderen Worten materiell den EU-Datenschutzstandard zu gewährleisten. Schwierigkeiten können sich für den im Inland ansässigen Nutzer allerdings ergeben, wenn er seine Datenschutzrechte in einer fremden Sprache gegenüber einer in einem EU-Staat ansässigen Stelle geltend machen will und hierzu die zuständige Aufsichtsbehörde (Kontrollstelle) identifizieren muss, um mit ihrer Hilfe seine Datenschutzrechte durchsetzen zu können.

Probleme werfen verteilte UC-Anwendungen auf, wenn die Daten verarbeitenden Stellen ihren Sitz in einem so genannten Drittstaat, d.h. außerhalb der EU haben, und deren Rechtsordnung keine hinreichenden mit dem EU-Datenschutzstandard vergleichbaren Datenschutzgarantien enthält. Bereits heute bilden Unternehmensnetze die internationalen Strukturen ihrer Organisation ab und ermöglichen eine kostengünstige und zeitliche Verlagerung personenbezogener Datenverarbeitungen in nahezu jedes Land der Erde.[407] Bei UC-Anwendungen, die ihrer Struktur nach bereits Netzwerkfähigkeit besitzen, wird sich die Internationalität der Verarbeitung als Normalfall bei der Planung und Optimierung entsprechender Geschäftsprozesse ergeben. Zwar können über besondere Instrumente wie Standardvertragsklauseln, Unternehmensrichtlinien und im Fall der USA über einen Beitritt zum Safe Harbor-Abkommen[408] kleinräumig Schutzstandards in ansonsten (datenschutzrechtlich) unsicheren Drittstaaten etabliert werden.[409] Es fragt sich aber, wer die Etablierung dieser Standards und ihre Einhaltung in einer Vielzahl international vernetzter UC-Systeme noch überprüfen und gegebenenfalls auch durchsetzen kann.[410] Sollen staatliche Kontrollen dies leisten, wird eine erheblich vereinfachte Zusammenarbeit der Kontrollstellen unumgänglich sein. Soll der Betroffene in die Lage versetzt werden, die Verarbeitung seiner Daten selbst zu kontrollieren, müssten auch hier schnellere, effektivere und kostengünstigere Strukturen der Rechtsdurchsetzung und -verfolgung geschaffen werden.[411]

Schutzprobleme treten auch auf, wenn die Übermittlung vermeintlich nicht personenbezogener, sondern nur objektbezogener Sensordaten in unsichere Drittstaaten erfolgt, dort der Personenbezug aber durch die Kombination mit anderen Datenbeständen im Wege eines Data Mining hergestellt wird. Ob die objektbezogenen Sensordaten bereits personenbeziehbar (§ 3 Abs. 1 BDSG) oder als faktisch anonymisiert (§ 3 Abs. 8 BDSG) gelten können, ist von dem zur Verfügung stehenden Zusatzwissen bzw. den Erkenntnismöglichkeiten der ver-

[407] Zur datenschutzrechtlichen Seite des Outsourcing siehe Hoenike / Hülsdunk, Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung?, MMR 2004, S. 788; Räther, Datenschutz und Outsourcing, DuD 2005, S. 461 ff.; Wagner, Outsourcing – mit Sicherheit, DuD 2005, S. 130.

[408] Zu den rechtlichen Möglichkeiten des Datentransfers in unsichere Drittstaaten siehe http://europa.eu.int/comm/justice_home/fsj/privacy/index_de.htm

[409] Siehe auch Büllesbach / Löss, Vertragslösung, Safe Harbor oder Privacy Code of Conduct, DuD 2002, 135 ff.; Dix, Datenschutzanforderungen an den Datenexport, DuD 6/2006 i.E.

[410] Probleme der Wirksamkeit des Safe Harbor-Abkommens im Hinblick auf die Schaffung eines angemessenen Schutzniveaus werden insbesondere auch in der Frage der Rechtsdurchsetzung gesehen, vgl. die Untersuchungen der EU-Kommission diesbezüglich, http://europa.eu.int/comm/justice_home /fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf.

[411] Dix, Datenexport, DuD 6/2006 (i.E.).

antwortlichen Stelle abhängig.[412] Ob die Verantwortlichen des Hintergrundsystems über das notwendige Zusatzwissen an Daten über den Betroffenen und die eingesetzten der Verfahren verfügen, wird sich jedoch ohne Kenntnis der Verfahren und des der Stelle verfügbaren Wissens letztlich nur schwer beurteilen lassen. Soweit UC-Systeme über Ländergrenzen hinweg, insbesondere unter Beteiligung von Drittstaaten außerhalb der Europäischen Union etabliert werden, besteht die Gefahr, dass die nationalen bzw. EU-weiten Schutzstandards unterlaufen werden. Dies kann nur vermieden werden, wenn der Übermittler beurteilen kann, ob die bei ihm erfassten Sensordaten personenbezogen verarbeitet werden können.

6.2.1.2 Outsourcing

Bei einer verteilten personenbezogenen Datenverarbeitung in UC-Systemen werden Verarbeitungen an Dritte delegiert werden, weil diese bspw. Rechenleistungen kostengünstig anbieten oder über benötigtes Know-how verfügen. Datenschutzrechtlich stellt sich die Frage, ob es sich bei der Vergabe solcher Verarbeitungen an externe Verarbeiter um eine Datenverarbeitung im Auftrag oder aber um eine Funktionsübertragung handelt.[413]

Im Fall einer Auftragsdatenverarbeitung muss die Verantwortung für die Verarbeitung der personenbezogenen Daten beim Auftraggeber liegen (§ 11 BDSG). Weitere Voraussetzungen sind die sorgfältige Auswahl eines geeigneten Auftragnehmers insbesondere auch im Hinblick auf die von diesem zu treffenden technischen und organisatorischen Maßnahmen,[414] eine schriftliche Auftragserteilung mit einer detaillierten Beschreibung der Verarbeitungsprozesse, der technisch-organisatorischen Maßnahmen und der eventuellen Unterauftragnehmer.[415] Bei einer Auftragsdatenverarbeitung ist der Auftragnehmer an die Weisungen des Auftraggebers gebunden und muss der Kontrolle durch seinen Auftraggeber unterliegen.[416] Im Wege einer Auftragsdatenverarbeitung wird der Auftragnehmer mit anderen Worten „an die Kette“ definierter Aufgaben in Form von Weisungen gelegt. Die rechtliche Folge ist, dass die Überlassung der zu verarbeitenden personenbezogenen Daten an den Auftraggeber keine Übermittlung an einen Dritten ist. Hat der Auftragnehmer seinen Sitz im EU-Binnenmarkt, dann findet auf ihn das jeweilige nationale Datenschutzrecht der Datensicherheit Anwendung.[417]

Soweit der Auftragnehmer über ein Entscheidungsermessen über das Ob oder das Wie der

---

[412] Zum Personenbezug: § 3 Abs. 1 BDSG; Dammann in: Simitis, BDSG, § 3, Rn. 36 ff.; 217. Saeltzer, Sind diese Daten personenbezogen oder nicht?, DuD 2004, S. 218 ff.

[413] Die Frage der Abgrenzung – ökonomisch motiviert – ist umstritten, vgl. nur Hoenike / Hülsdunk, Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung?, MMR 2004, S. 788; Räther, Datenschutz und Outsourcing, DuD 2005, S. 461 ff.; Wagner, Outsourcing – mit Sicherheit, DuD 2005, S. 130. alle m.w.N.

[414] § 11 Abs. 2 S. 1 BDSG.

[415] § 11 Abs. 2 S. 2 BDSG.

[416] § 11 Abs. 2 S.4, Abs. 3 S. 1 BDSG.

[417] Art. 17 Abs. 3, Zweiter Spiegelstrich EG-Datenschutzrichtlinie, Dammann in: Simitis, BDSG-Kommentar, 5. Aufl., § 1, Rn. 208.

ihm übertragenen Verarbeitungsvorgänge verfügt, kann nicht mehr von einer Datenverarbeitung im Auftrag nach § 11 BDSG ausgegangen werden. In diesem Fall liegt eine Funktionsübertragung an einen Dritten und damit eine Übermittlung im datenschutzrechtlichen Sinne vor. Die Verarbeitungsvorgänge müssen dann auf Basis einer informierten Einwilligung des Betroffenen oder einer Erlaubnisvorschrift erfolgen.[418] Gleichwohl wird es im Fall einer verteilten Verarbeitung für den Betroffenen im Einzelfall schwierig werden, die für die Verarbeitung seiner Daten verantwortliche Stelle zu bestimmen.

Rechtlich ist die Frage der Verantwortlichkeit zwischen der Daten verarbeitenden Stelle und dem Betroffenen geklärt, wenn seine Daten im Wege einer Auftragsdatenverarbeitung verarbeitet werden. Hier ist der Auftraggeber gegenüber dem Betroffenen für die Rechtmäßigkeit der Verarbeitung verantwortliche Stelle und damit Ansprechpartner für den Betroffenen. In dieser Konstellation steht und fällt das faktische Datenschutzniveau aber mit Art und Intensität der Ausübung der Kontrollbefugnis des Auftraggebers. Eine Vielzahl von Auftragsverhältnissen erhöht seinen Aufwand, um die erforderliche Kontrolldichte gegenüber den Auftragnehmern gewährleisten zu können. Auch könnten die Kosten für die erforderlichen Kontrollen der Auftragnehmer vor allem im Ausland den ökonomischen Vorteil des Auftraggebers schmälern, so dass sie zu Lasten der Kontrolldichte bewusst niedrig gehalten werden.

In der Praxis werden in den derzeit üblichen Outsourcing-Modellen häufig Funktionalitäten einschließlich eines Entscheidungsermessens an Dritte übertragen, die dann datenschutzrechtlich als eine Funktionsübertragung zu bewerten sind. Das Outsourcing erfolgt in diesem Fall im Wege einer normalen Übermittlung personenbezogener Daten, die zu ihrer Zulässigkeit einer Einwilligung des Betroffenen oder aber einer gesetzlichen Erlaubnisvorschrift bedarf. Bei einer Funktionsübertragung im Rahmen einer UC-Anwendung wird für den Betroffenen regelmäßig ein Transparenzproblem zu lösen sein. Ohne Unterstützung wird der Betroffene kaum in der Lage sein festzustellen, wer in der Kette der Beteiligten seine Daten verarbeitet hat bzw. an welcher Stelle ein Verstoß gegen seine Datenschutzrechte aufgetreten ist. Diese Intransparenz beschränkt nicht nur seine Möglichkeiten, die Verarbeitung seiner Daten nachzuvollziehen, sondern erschwert auch den Nachweis der Verletzung seiner Rechte.

6.2.1.3 Durchsetzung von Vorgaben

Rechtliche Vorgaben sind letztlich nur dann wirksam, wenn sie effektiv kontrolliert und auch durchgesetzt werden können. Das Bundesdatenschutzgesetz sieht zu diesem Zweck eine Instanz der Selbstkontrolle für Unternehmen und Behörden in Form betrieblicher bzw. behördlicher Datenschutzbeauftragter vor.[419] Als staatliche Kontrollinstanz überwachen die Datenschutzbeauftragten bzw. die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich die Verarbeitung der verantwortlichen Stellen.[420] Darüber hinaus können die Betrof-

[418] § 4 Abs. 1 BDSG.

[419] § 4f BDSG.

[420] § 38 BDSG.

fenen gegenüber der verantwortlichen Stelle selbst ihre Rechte geltend machen. Der Gesetzgeber setzt insoweit auf eine Selbstkontrolle der Verarbeitung durch das betroffene Individuum, das durch Informationspflichten der verantwortlichen Stelle[421], Auskunftsrechte[422] und Einwilligungserfordernisse[423] bei der Kontrolle seiner personenbezogenen Daten unterstützt werden soll. Darüber hinaus kann der Betroffene unter den gegebenen Voraussetzungen Schadensersatzansprüche geltend machen.[424]

Anwendungen des Ubiquitous Computing sind bereits strukturell auf eine geringe Sichtbarkeit der Verarbeitungsprozesse gegenüber dem Betroffenen angelegt.[425] Sie funktionieren in der Regel über eine Vielzahl von Datenverarbeitungen, die von dem Betroffenen nur schwer nachzuvollziehen sind, so dass unter diesen Bedingungen eine Kontrolle der UC-Systeme durch den Betroffenen und eine selbst bestimmte Entscheidung nur schwer umzusetzen ist. Die Grundprinzipien des Ubiquitous Computing und der informationellen Selbstbestimmung sind unter diesen Bedingungen gegenläufig. Ein Widerspruch, der sich voraussichtlich nur durch Kompromisse bei der Umsetzung dieser Strukturprinzipien auflösen lässt.

Das Konzept der Aufsichtsbehörden als Instanz zur Kontroll- und Rechtsdurchsetzung ist dem Ursprung des Datenschutzes als Schutzrecht des Bürgers gegen eine staatliche Datenverarbeitung geschuldet. Es funktioniert bei einer begrenzten Anzahl von lokal verantwortlichen Stellen, wenn sie über das erforderliche Personal verfügen. Für den zahlenmäßig grundsätzlich unbegrenzten nicht-öffentlichen Bereich, in dem eine Vielzahl der Anwendungen Ubiquitous Computing zu erwarten sind, kann eine staatliche Struktur der Datenschutzaufsicht nur eine stichprobenartige oder anlassbezogene Kontrolltätigkeit leisten.[426] Der exponentielle Zuwachs von Verarbeitungen in UC-Systemen und die Komplexität der einzelnen Verfahren wird die Effektivität dieser Aufsichtsform weiter reduzieren. Instanzen der Selbstkontrolle wie dem betrieblichen Datenschutzbeauftragten kommt daher für die Gewährleistung des Datenschutzes in den Organisationen eine noch wichtigere Rolle zu. Ein weiteres Instrument der präventiven Datenschutzkontrolle ist die Vorabkontrolle, die der betriebliche Datenschutzbeauftragte nach § 4 d Abs. 5 und 6 BDSG bei besonderen Risiken für die Rechte und Freiheiten der Betroffenen vor der Verarbeitung durchzuführen hat.

Im Übrigen können die Betreiber von UC-Systemen gegenüber den Betroffenen auch im Wege der Selbstverpflichtung Art und Umfang ihrer Datenerhebung und –verarbeitung beschränken. Allerdings ist die rechtliche Bindungswirkung derartiger Selbstverpflichtungen jedoch schwach, weil sie den Betroffenen in der Regel keine gerichtlich durchsetzbaren Ansprüche vermitteln kann. Zudem wird die Bereitschaft zur Selbstverpflichtung in dem Maße sinken, in dem der wirtschaftliche Wert der in UC-Anwendungen generierten und mit ande-

[421] z.B. § 33, § 28 Abs. 4, § 4 a BDSG.

[422] § 34 BDSG.

[423] § 4 Abs. 1 BDSG.

[424] § 7 BDSG.

[425] Prinzip des Calm Computing, s.o. Kapitel 1.

[426] Auch wenn anlassfreie Prüfungen gem. § 38 BDSG zulässig sind.

ren verknüpften Daten wächst. Gleichwohl lässt sich die Verbindlichkeit derartiger Selbstverflichtungen bspw. auch dadurch steigern, dass ihre Einhaltung in Form von Audits durch unabhängige Dritte regelmäßig überprüft und öffentlich bestätigt wird. Gewährsträger der Normbefolgung ist in diesen Fällen dann nicht die Aufsichtsbehörde, sondern die Sorge des Unternehmens vor einem wirtschaftlich nicht unbedeutenden Imageschaden. Zum anderen kann ein Verstoß gegen eine öffentliche und damit werbewirksame Selbstverpflichtung als Verstoß gegen die Regeln eines fairen Wettbewerbes auch von den Konkurrenten bzw. entsprechenden klagebefugten Verbänden gerichtlich geahndet werden.

6.2.1.4 Bewegungsprofile

UC-Systeme, die mehr oder weniger flächendeckend eingesetzt werden und dabei permanent Produkte und deren Besitzer identifizieren, erstellen durch den regelmäßigen Identifikationsvorgang Bewegungsprofile der Betroffenen. Sie ermöglichen damit eine räumliche und zeitliche Überwachung von Menschen mit tiefgreifenden Folgen für das informationelle Selbstbestimmungsrecht der Betroffenen.

Ein Beispiel liefert die RFID-Technik.[427] Sind Produkte des täglichen Lebens dauerhaft mit RFID gekennzeichnet, so werden sie aufgrund einheitlicher Standards von jedem Inhaber eines Lesegerätes ausgelesen werden können. In diesem Fall kann eine Profilbildung und Auswertung aber auch über verschiedene verantwortliche Stellen hinweg erfolgen.[428] Denkbar ist auch, dass ein Verbraucher mit über RFID gekennzeichneten Alltagsgegenständen (so genannten „getagten Objekten“) ein beliebiges Geschäft betritt, in dem das Lesesystem des Geschäftsinhabers ihn an Hand seiner Kunden- oder Zahlungskarte identifiziert und zusätzlich während seines Aufenthaltes auch die Kennnummern der getagten Objekte erfasst, ausliest, speichert und seiner Person zuordnet.

Die Problematik der Profilbildung verschärft sich, wenn aktive RFID-Tags aus Produkten erfasst werden, die der betroffene Verbraucher in der Vergangenheit in diesem oder anderen Geschäften erworben hat. Der Geschäftsbetreiber würde in diesem Fall der Person des ihm nun bekannten Kunden die Objektnummern zahlreicher Produkte zuordnen können. Unter der Voraussetzung, dass das System des Geschäftsbetreibers diese Kennnummern interpretieren kann[429], kennt es nicht nur die Identität des Verbrauchers, sondern verfügt

[427] Zu den vielfältigen Datenschutzfragen von RFID: Hansen / Wiese, Gateway, RFID – Radio Frequency Identification, DuD 2004, S. 109, Barthel, RFID-Anwendungen im Betrieb und bei Arbeitnehmerdaten, DANA 03/2004, S. 5, Kelter, Widmann, Radio Frequency Identification - RFID , DuD 2004, S. 331, Müller, Ist das Auslesen von RFID-Tags zulässig? – Schutz von RFID-Transponderinformationen durch § 86 TKG, DuD 2004, S. 215, Müller, Handy, RFID und Datenschutzrecht, Risiken, Schutzbedarf und Gestaltungsideen, DuD 2004, S. 655, Holznagel / Bonnekoh, Radio Frequency Identification – Innovation vs. Datenschutz?. MMR 2006, S. 17, Hülsmann, RFIDs – Bleibt der Datenschutz auf der Strecke?, DANA 04/2004, S. 11.

[428] Dies setzt Nachverfolgungsmöglichkeiten von Nutzern von Webseiten über Bannerwerbung für die reale Welt um. Strukturell beobachtet hier aber nicht eine Stelle (Bannervermarkter) an vielen Orten (Webseiten) sondern es entstehen viele Profile verschiedener Verantwortlicher, die aber einfach zusammenführbar sind.

pretieren kann[429], kennt es nicht nur die Identität des Verbrauchers, sondern verfügt auch über die Informationen zu den Dingen, die er bei sich trägt. Diese Auswertung erfasst also zum einen die Objekte, die der Betroffene bereits mit sich geführt hat, als er den Laden betrat, kann aber auch die Objekte betreffen, die er während seines Aufenthaltes in dem Geschäft in die Hand genommen hat. An der Auswertung dieser Informationen wird der Geschäftsbetreiber auch ein wirtschaftliches Interesse haben, weil er auf diese Weise über die Objekte Indikatoren für ein individuelles Profil der Eigenschaften und Vorlieben, aber auch der finanziellen Leistungsstärke der jeweiligen Person erstellen kann. Aber selbst wenn der Geschäftsbetreiber keine der „fremden" Objektnummern interpretieren kann, so ermöglichen ihm diese Informationen, den Verbraucher bei seinem nächsten Besuch im Geschäft anhand der von ihm bereits gespeicherten Objektinformationen zu identifizieren.

Für eine Erhebung von fremden Objektinformationen und ihre Zuordnung zur Person ihres Trägers bedarf der Geschäftsbetreiber als der hierfür verantwortlichen Stelle einer Einwilligung des Betroffenen.[430] Mangels eines Vertragsverhältnisses über die bereits gekauften Objekte scheidet § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Rechtsgrundlage aus. Nr. 2 dieser Vorschrift ist nicht einschlägig, weil die schutzwürdigen Interessen des Betroffenen bei einer heimlichen Erfassung seiner Objekte und ihrer Zuordnung zu seiner Person in jedem Fall die Interessen des Geschäftsbetreibers überwiegen werden.[431] Die gesetzlichen Tatbestände der Datenerhebung und –verarbeitung rechtfertigen also keine heimliche und automatisierte Erhebung fremder Objektinformationen über den Betroffenen ohne seine aktive Mitwirkung.

Ist aber eine Einwilligung des Betroffenen erforderlich, bevor die Kennnummern seiner Objekte personenbezogen ausgelesen werden, so setzt dies ein Einwilligungsmanagement durch die auslesenden Stellen voraus, d.h. die Betroffenen müssen angesprochen, informiert und um ihre Einwilligung gebeten werden. Ein solches Einwilligungsmanagement erfordert zudem eine Steuerung der Lesegeräte, weil für den Fall, dass Betroffene ihre Einwilligung nicht erteilen, das Auslesen ihrer Objekte unterbleiben muss. Kann das Auslesen der Kennnummern getagter Objekte aber nicht gezielt auf die Objekte und Stellen beschränkt werden, die von der datenschutzrechtlichen Einwilligung des Kunden oder einem gesetzlichen Erlaubnistatbestand umfasst sind, dann bleibt unter Datenschutzgesichtspunkten nur die Möglichkeit einer regelmäßigen Deaktivierung der RFID-Tags[432] nach Abschluss des individualisierten Kaufvorgangs. Die Konsequenz ist, dass der Nutzung von Kennnummern je Objekt aus den RFID-Tags bspw. für Zwecke der Gewährleistung oder im Rahmen eines Life-Cycle-

[429] Was insbesondere durch einen Zugriff auf die Datenbanken des standardisierten globalen EPC-Netzwerks unproblematisch möglich ist.

[430] Holznagel / Bonnekoh, MMR 2006, 21. Siehe auch Kapitel 3 unter rechtliche Bestimmungsfaktoren.

[431] Siehe auch Holznagel / Bonnekoh, Radio Frequency Identification – Innovation vs. Datenschutz?, MMR 2005, 20 f.

[432] Das Vertrauensproblem nicht deaktivierter RFID haben auch Unternehmen erkannt, siehe Heise Newsticker: IBM schlägt datenschutzgerechte RFID-Chips vor, http://www.heise.de/newsticker/meldung/70778 (13.03.2006).

Managements deutliche Grenzen gesetzt sind.[433]

6.2.2 Funktionale Risiken der UC-Systeme

6.2.2.1 Sensortechnik

Neben den genannten strukturellen Problemen von UC-Anwendungen für das informationelle Selbstbestimmungsrecht ergeben sich auch aus den einzelnen Funktionen der UC-Systeme Risiken für die informationelle Selbstbestimmung.[434]

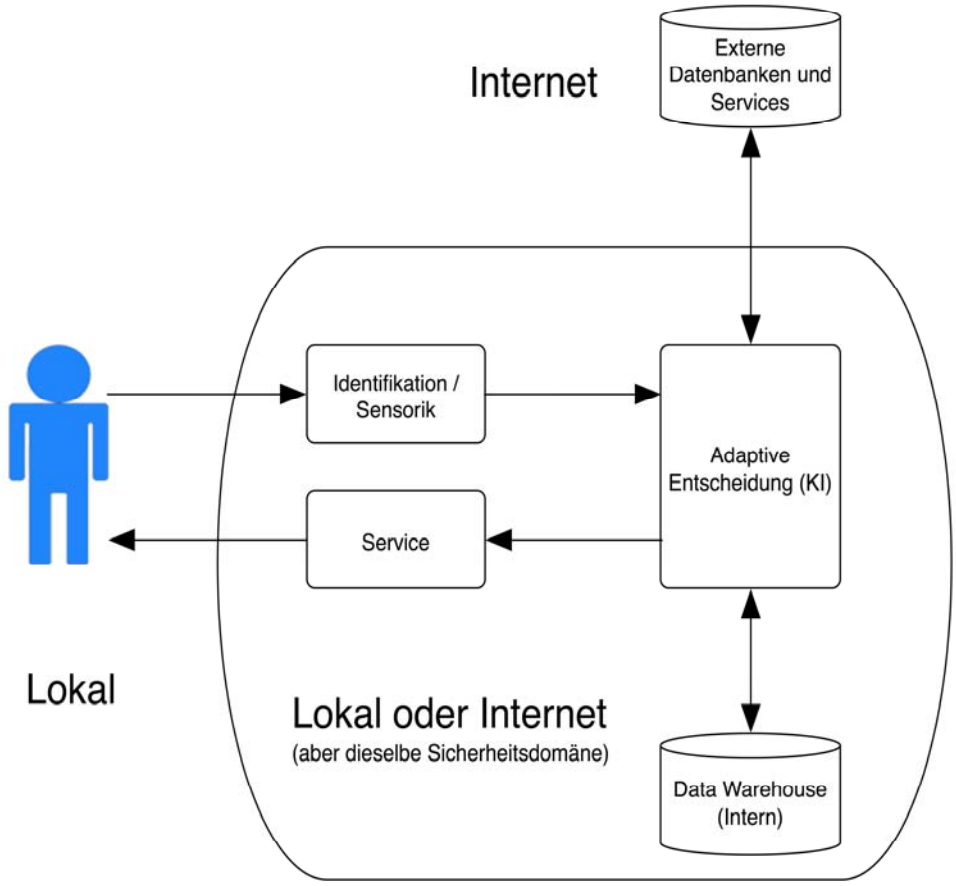


Abbildung 29: Adaptives UC-System (vergl. Kap. 1.2)

Die in dieser Studie beschriebenen UC-Anwendungen beinhalten fast durchgängig eine Form von Sensor-Technik, die (personenbezogene) Daten erfasst. Die Erfassung personenbezogener Daten bedarf einer Einwilligung des Betroffenen oder einer gesetzlichen Erlaubnisvorschrift. Beides erfordert in der Regel eine umfassende Information des Betroffenen

[433] So auch mit nahezu einhelligem Ergebnis (mit Ausnahme des Einzelhandels) die Ergebnisse der Konsultation der Art. 29 Gruppe: Ergebnisse der öffentlichen Anhörung zum Arbeitspapier 105 der Art. 29 Arbeitsgruppe zum Thema Datenschutz und RFID-Technologie, http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_de.pdf

[434] Siehe zu dem generischen Modell von UC-Anwendungen Kapitel 1.

über den Verarbeitungsvorgang.[435]

Bei UC-Anwendungen wird der Erfassungsvorgang von dem Betroffenen oft nicht wahrgenommen, wenn er nicht durch ein besonderes Signal darauf hingewiesen wird. Die Unsichtbarkeit der Erfassung ist ein Design-Merkmal der Technik und insofern kein behebbarer Fehler. Das klassische Beispiel ist das Auslesen von RFID-Tags. Im Gegensatz zum manuellen Auslesen eines Barcodes an der Kasse durch die Kassiererin soll das Auslesen eines RFID-Tags weder sichtbar erfolgen noch benötigt es einen physischen Kontakt, durch den der Betroffene auf den Vorgang aufmerksam würde. Allenfalls eine gewisse physische Nähe zum Lesegerät kann noch notwendig sein, je nachdem was für ein RFID-Tag verwendet wird. Die Reichweite der ubiquitären Sensortechnik variiert stark.[436] Im Übrigen können die Objekte bzw. ihre Träger durch die Führung der Laufwege vergleichbar dem Weg zur und an der Kasse im Ladengeschäft in ausreichender Nähe an den Lesegeräten vorbeigeführt werden, ohne dass der Lesevorgang für sie erkennbar wäre.

Zudem sind die Lesegeräte meist unsichtbar in die Gegenstände der Umgebung integriert. Eine Kennzeichnungspflicht für solche Lesegeräte könnte den Kunden zwar über die Möglichkeit eines Auslesevorgangs informieren, ob eine solche im Einzelfall aber stattfindet und welche Daten erfasst werden, kann der Betroffene einem derartigen allgemeinen Hinweis noch nicht entnehmen. In einzelnen Anwendungen können Displays weiterhelfen, die die Auslesevorgänge und die Daten anzeigen. Mit der Menge an Auslesevorgängen wird aber die Aufmerksamkeit der Betroffenen abnehmen, diese Hinweise wahrzunehmen und zu bewerten.[437] Andere Technologien allgegenwärtiger Datenverarbeitung wie z.B. Smart Dust[438] werden derartige Kennzeichnungen schon auf Grund ihrer Funktionsweise nicht ermöglichen. Eine Kennzeichnungspflicht der Lesegeräte und Auslesevorgänge würde dem Transparenzdefizit der Betroffenen in ubiquitären Anwendungen also nur in Einzelfällen abhelfen können.

Datenschutzrechtlich ist zusätzlich zu berücksichtigen, dass die sensorisch erhobenen Daten wie z.B. die auf einem RFID gespeicherte Nummer eines Produktes für sich allein noch über keinen direkten Personenbezug verfügen. Über das Lesegerät erfolgt im Hintergrundsystem zunächst nur eine personenbeziehbare Profilbildung, die aber über den Auslesekontext, das Zahlungsmittel, die Kundenkarte oder die körperliche Nähe wie z.B. ein in ein Kleidungsstück eingenähtes RFID in Verbindung mit einer Videoüberwachung oder andere Kombinationen von Daten auf eine Person zurückzuführen sind und damit als Bestandteil eines Profils z.B. auf das Konsumverhalten, Vorlieben etc. der Person schließen lassen. Solche Daten fallen

[435] Vgl. § 4a BDSG, § 4 Abs. 1 und 2 TDDSG für die Einwilligung, § 33 , § 28 Abs. 4 S. 2 BDSG zu sonstigen Informationspflichten, § 6 b Abs. 2 zu besonderen Kennzeichnungspflichten bei der Videoüberwachung, deren Eigenschaft der permanenten (optischen) Überwachung der sensorischen Überwachung des RFID strukturell sehr nahe kommt. Siehe auch Eisenberg / Puschke / Singelnstein, Überwachung mittels RFID-Technologie, ZRP 2005, S. 9 (12).

[436] Siehe oben Kapitel 2 dieser Studie.

[437] Zur Aufmerksamkeitsökonomie siehe Kapitel 5 dieser Studie.

[438] Zum Smart Dust siehe Kapitel 1.

nach der Definition des § 3 Abs. 1 BDSG unter den Begriff der personenbezogenen Daten, da es sich um Einzelangaben über die persönlichen oder sachlichen Verhältnisse einer *bestimmbaren* Person handelt.[439]

Das Datenschutzrecht geht grundsätzlich von einer Relativität des Personenbezugs aus, d.h. die Person ist für denjenigen, der über das entsprechende Zusatzwissen verfügt, bestimmbar.[440] Von einem solchen Personenbezug ist immer auszugehen, wenn die Informationen über die Zuordnung der Person aus einer allgemein zugänglichen Quelle stammen. Diese Voraussetzung liegt bereits dann vor, wenn der Träger der RFID-Tags als Person in der Öffentlichkeit jederzeit identifiziert werden kann. Im Übrigen gilt als Maßstab für die Bewertung eines Personenbezuges, dass die „legale Bekanntgabe" des hierfür erforderlichen Zusatzwissens über Einzelpersonen „nach sozialüblichen Maßstäben nicht ausgeschlossen werden kann".[441] Sozialüblich ist insbesondere, dass sich die betreffende Person in der Öffentlichkeit bewegt und kommuniziert, d.h. sich selbst bspw. in der sozialen Interaktion, aber auch durch Vorlage ihrer Kunden- oder Zahlungskarte zu erkennen gibt.[442] Weil dies regelmäßig nicht nur nicht auszuschließen, sondern anzunehmen sein wird, sind die Kennnummern der RFID-Tags in oder an den Objekten in Hinblick auf ihren Träger praktisch immer personenbeziehbare Daten.

Die Frage des Personenbezugs von Daten, die für das Erbringen technischer Leistungen erforderlich sind, wurde bereits von den Autoren des Gutachtens zur Modernisierung des Datenschutzrechts diskutiert.[443] Sie schlagen eine Unterscheidung nach Datenverarbeitungsvorgängen mit und ohne gezielten Personenbezug vor.[444] Daten ohne einen gezielten Personenbezug, die nach einer solchen Neukonzeption des Datenschutzrechts ohne weitere Einschränkungen zu verarbeiten sein sollen, würden verwendet werden, um eine technische Kommunikation zwischen automatisch tätigen Maschinen oder Verfahren zur Suche von Informationen zu ermöglichen. Unter diese Kategorie würden auch die von den Sensoren der Lesegeräte regelmäßig erfassten Objektdaten fallen. Jedoch ist die von den Gutachtern vorgeschlagene Kategorisierung unter mehreren Gesichtspunkten problematisch und für das Schutzziel des Datenschutzes nicht angemessen:

Die Gutachter weisen zu Recht auf die Doppelnatur solcher Daten hin, die insbesondere dann ein hohes Risiko für Persönlichkeitsrechtsverletzungen bergen, wenn sie das technische System verlassen und für andere Zwecke verwendet werden.[445] UC-Systeme, die in ihrem Aufbau dem dargestellten generischen Modell folgen, müssen grundsätzlich als offene

---

[439] So auch Eisenberg / Singelnstein / Puschke, Überwachung mittels RFID-Technologie, ZRP 2005, S. 9 (10) zur Personenbeziehbarkeit der erfassten Daten.

[440] Dammann in: Simitis, BDSG, § 3, Rn. 32.

[441] Ebd., § 3, Rn. 36.

[442] Ebd., § 3, Rn. 36.

[443] Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, Berlin 2001.

[444] Ebd, S. 113.

[445] Ebd, S. 114.

Systeme betrachtet werden, da - wie bereits dargestellt - Teilkomponenten von unterschiedlichen Verantwortlichen erbracht werden können. Die Zweckbindung in solchen Systemen zu kontrollieren, ist kaum möglich. Aus demselben Grund ist es zweifelhaft, ob die Unterteilung der Datenverarbeitung in solche mit einem und solche ohne einen gezielten Personenbezug für UC-Systeme praktisch umzusetzen ist und nicht zusätzliche Schutzlücken öffnet.

Zusätzliche Kategorien mit abweichenden Schutzstandards erhöhen die Komplexität des Regelungssystems, erschweren die Transparenz für die Betroffenen sowie die Rechtsanwendung. Sie werden die verantwortlichen Stellen im Übrigen dazu motivieren, Verarbeitungen möglichst in die privilegierte Klasse der Daten ohne einen gezielten Personenbezug einzuordnen. Diesen Nachteilen ließe sich entweder nur durch eine präzise, aber komplexe Regelung in der Art einer Liste von zulässigerweise zu verwendenden Daten („Listenprivileg“) oder aber durch eine auslegungsbedürftige Generalklausel begegnen. Gegen ein Listenprivileg spricht bereits, dass die in UC-Systemen zu verarbeitenden Daten angesichts der Vielzahl von Anwendungen nicht abschließend bestimmt werden können. Gegen eine generalklauselartige Bestimmung spricht, dass sie für den Betroffenen die Durchsetzung seiner Datenschutzrechte nicht erleichtert, sondern erschwert, weil er im Zweifelsfall die Beweislast tragen wird, dass die erhobenen Daten gezielt über einen Personenbezug verfügen.

Vor diesem Hintergrund entspricht die konventionelle Auslegung des Begriffs der personenbezogenen Daten nach wie vor dem Schutzgedanken des Datenschutzes, denn sie überlässt mit ihrem weiten Anwendungsbereich die Nachweispflicht für die Zulässigkeit der Datenverarbeitung grundsätzlich der verantwortlichen Stelle und nicht dem Betroffenen. Zudem ist die von den Gutachtern befürchtete Inflation datenschutzrechtlicher Auskunftsansprüche angesichts der bereits heute zu vernachlässigenden Zahl an tatsächlichen Auskunftsbegehren praxisfremd.[446] In Frage gestellt werden sollte im Übrigen auch nicht die Informationspflicht der verantwortlichen Stelle, die technisch bedingt Sensordaten erhebt, sondern allenfalls die Art und Weise dieser Verpflichtung nachzukommen.

Die Autoren des Gutachtens erwarteten für eine Welt vernetzter und allgegenwärtiger Datenverarbeitung, dass immer öfter Daten verarbeitet werden, für die zu diesem Zeitpunkt unbekannt ist, ob sie sich auf eine bestimmte Person beziehen, auf welche Personen sie sich beziehen oder welchen Personen sie künftig zugeordnet werden.[447] Gleichwohl soll diesen Daten nach Ansicht der Gutachter ein Schutz nach grundsätzlichen datenschutzrechtlichen Prinzipien zukommen, wenn zu erwarten ist, dass ein Personenbezug hergestellt wird oder werden kann. Die dargestellte Problematik erweist sich bei einer Betrachtung der konkret werdenden Einsatzumfelder von UC in besonderer Weise als relevant. In UC-Systemen werden häufig zunächst objektbezogene Daten erfasst, die erst später durch Erkenntnisse aus anderen Sensoren oder Hintergrunddatenbanken personenbeziehbar werden. Eine unreglementierte Sammlung, Speicherung und Verbreitung würde eine erhebliche Schutzlücke darstellen, wenn nachträglich - auch durch Dritte - ein Personenbezug hergestellt wird. Re-

[446] Vgl. ULD, Verbraucherdatenschutz, Gutachten, April 2006.

[447] Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, Berlin 2001, S. 61.

gelmäßig wird erst in Kenntnis der Funktionsweise eines solchen UC-Systems eine grundsätzliche Personenbeziehbarkeit der relevanten Sensordaten festzustellen sein. Über diese Kenntnis verfügt jedoch der Betreiber des Hintergrundsystems, der entweder einen Personenbezug vermeiden muss oder aber nach den allgemeinen Regeln des Datenschutzrechts als verantwortliche Stelle zur Information der Betroffenen und zur Rechtmäßigkeit der Verarbeitung verpflichtet ist. Es ist gerade Sinn und Zweck des datenschutzrechtlichen Erlaubnisvorbehaltes, die Beweislast für die Rechtmäßigkeit der Datenverarbeitung der für den Personenbezug verantwortlichen Stelle zuzuordnen. Insofern ist auch für Sensordaten einer Vielzahl von UC-Systemen davon auszugehen, dass regelmäßig Daten mit einem (gezielten) Personenbezug verarbeitet werden.

Ein Beispiel für die strukturell mit Anwendungen des Ubiquitous Computing einhergehenden Transparenzdefizite und die daraus resultierenden Folgen für die informationelle Selbstbestimmung ist die Einwilligung in die personenbezogene Datenverarbeitung. Der Betroffene muss grundsätzlich wissen, in welchen Verwendungszweck seiner Daten er einwilligt.[448] Pauschal gehaltene Einwilligungserklärungen in eine personenbezogene Datenverarbeitung zu nicht näher bestimmten Verwendungszwecken sind unwirksam.[449] Entsprechendes gilt auch für eine Einwilligung in die Verarbeitung personenbezogener Daten, mit der die Erhebung und Verarbeitung personenbezogener Objektdaten in einem definierten Raum legitimiert werden soll. Die Einwilligung kann sich immer nur auf definierte Verwendungszwecke gegenüber benannten verantwortlichen Stellen beziehen. Diese Anforderung ist aber kaum zu erfüllen, wenn die Objektdaten von unzähligen Stellen ausgelesen und verarbeitet werden.

Die Umsetzung ständiger Einwilligungserklärungen mit entsprechenden Informationen über Art und Umfang der einzelnen Verarbeitungen droht die Komfortvorteile der ubiquitären Anwendungen zunichte zu machen. Das Strukturmerkmal „calm“ des Ubiquitous Computing und das Grundprinzip Transparenz stehen in einem Spannungsverhältnis. Will man die Vorteile ubiquitärer Anwendungen ermöglichen, so wird dies nur durch Kompromisse bei der Umsetzung der Anforderung an eine informierte Einwilligung des Betroffenen möglich sein. Zugeständnisse werden aber ihre Grenzen dort finden müssen, wo den Betroffenen eine Ausübung ihres informationellen Selbstbestimmungsrechts nicht mehr sinnvoll möglich ist. Zudem steht bei einem hohen Verbreitungsgrad an UC-Umgebungen auch die Freiwilligkeit der Einwilligung[450] in Frage, insbesondere wenn bestimmte Dienstleistungen oder Produkte für die Betroffenen, die derartige Datenverarbeitungen ablehnen, nicht mehr zur Verfügung stehen. Die datenschutzrechtliche Notwendigkeit einer Einwilligung wirft angesichts dieser Anforderungen die grundsätzliche Frage auf, ob eine UC-Umgebung von dem Betroffenen überhaupt genutzt werden kann.

[448] Simitis in: Simitis, BDSG § 4 a, Rn. 74 ff.; § 4 a Abs. 1 und 3 BDSG, § 4 Abs. 1 und 2 TDDSG.

[449] ebd., § 4 a, Rn. 74.

[450] Vgl. § 4 a BDSG, § 3 Abs. 4 TDDSG.

6.2.2.2 Datentransport

Die von den Lesegeräten bzw. Sensoren erhobenen Daten werden zur Weiterverarbeitung an ein Hintergrundsystem übermittelt. Da diese Informationen für bestimmte Nutzergruppen bereits bei der Erhebung personenbezogen sind, unterliegt die für die Verarbeitung dieser Daten verantwortliche Stelle der Verpflichtung nach § 9 BDSG, durch technisch-organisatorische Maßnahmen für eine angemessene Datensicherheit zu sorgen. Sie hat insbesondere die technisch-organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten.[451] Hierzu gehören nach der Anlage zu § 9 BDSG insbesondere die Zutrittskontrolle, die Zugangskontrolle, die Zugriffskontrolle, die Weitergabekontrolle, die Eingabekontrolle, die Auftragskontrolle, die Verfügbarkeitskontrolle und die Sicherstellung des Trennungsprinzips. Die Datensicherheit ist insofern notwendige Voraussetzung für die Möglichkeit, einen angemessenen Datenschutz gewährleisten zu können.

Kapitel 7 legt ausführlich dar, welche strukturellen Probleme die verschiedenen Technologien des Ubiquitous Computing für die Datensicherheit in sich bergen. Demnach weisen die diversen Systeme eine Reihe von erheblichen Schutzlücken auf, die eine Verarbeitung personenbezogener Daten unter Datenschutzgesichtspunkten häufig ausschließen. Die Erfüllung von Sicherheitsanforderungen wird im Einzelfall für jedes konkrete UC-System zu prüfen sein. Dies ist auch schon deswegen geboten, weil die Sicherheitsanforderungen bspw. für die Übermittlung personenbezogener Daten davon abhängig sind, welche Techniken zwischen den Lesegeräten bzw. Sensoren und den Hintergrundsystemen eingesetzt werden. Darüber hinaus ist jeweils zu prüfen, ob in einer UC-Anwendung unterschiedliche Übermittlungsverfahren eingesetzt werden.

Die übertragenen Daten sind sowohl gegenüber einem Zugriff Dritter als auch gegenüber den an der Übermittlung Beteiligten zu schützen. Gegen einen Missbrauch personenbezogener Daten kann unter der Voraussetzung, dass für die Übertragung ein Telekommunikationsdienst eingesetzt wird, zumindest rechtlich das Telekommunikationsgeheimnis einen gewissen Schutz bieten.[452] Zudem gewährleistet das Strafrecht gegenüber Personen, die personenbezogene Daten aus einer UC-Anwendung rechtswidrig zur Kenntnis nehmen, einen strafrechtlichen Schutz. Fraglich ist jedoch, ob und inwieweit angesichts der geschilderten Probleme bei der Nachvollziehbarkeit von Handlungen in UC-Systemen (Revisibilität) und der fehlenden sicheren Authentifizierung der einbezogenen Geräte,[453] Täter ermittelt und eine Straftat nachgewiesen werden können.

---

[451] Ernestus / Geiger in: Simitis, BDSG, § 9 Rn. 2 f.

[452] Art. 10 GG, § 88 TKG, § 206 StGB; Müller, Jürgen: Ist das Auslesen von RFID-Tags zulässig? – Schutz von RFID-Transponderinformationen durch § 86 TKG, DuD 2004, S. 215, Ohlenburg, Anna, Der neue Telekommunikationsdatenschutz, MMR 2004 S. 431; siehe Kapitel 3.4.3.5.3.

[453] Siehe Kapitel 7 dieser Studie.

6.2.2.3 Hintergrunddatenbanken

Unter Datenschutzgesichtspunkten von erheblicher Bedeutung ist, wenn die über Lesegeräte bzw. Sensoren von UC-Systemen erfassten Daten in Hintergrunddatenbanken mit anderen Informationen über ihre Träger verknüpft werden.[454] Die Verbindung erfolgt bspw. über die Objektnummer in dem RFID-Tag in Verbindung mit den Kontaktinformationen des Kunden, die aus seiner Kunden- oder Zahlungskarte ermittelt worden sind, und bildet das Ausgangsmaterial für die Erstellung und Auswertung eines Nutzungs- bzw. Kundenprofils. Das Erheben, Verarbeiten oder Nutzen derartiger personenbezogener Daten unterliegt jedoch dem datenschutzrechtlichen Erlaubnisvorbehalt.[455] Dabei ist zu beachten, dass Kundenprofile außerhalb der Erfüllung eines konkreten Vertragsverhältnisses grundsätzlich einer gesonderten Einwilligung des Betroffenen bedürfen.[456]

In UC-Anwendungen ist zu erwarten, dass eine Vielzahl personenbezogener Datenbanken betrieben wird, in denen ausgelesene Objektdaten für Zwecke einer nutzungs- und kundenbezogenen Auswertung vorgehalten und schließlich auch den Trägern der Objekte zugeordnet werden, sobald sie authentifiziert werden können.[457] Für den Betroffenen ist regelmäßig nur schwer zu erkennen, welche verantwortliche Stelle welche Informationen seiner Objekte ausliest und zu welchem Zweck speichert und schließlich auch verarbeitet und nutzt. Zusätzliche Probleme ergeben sich, wenn in dem Hintergrundsystem Objektdaten aus der Vergangenheit gespeichert werden, die nun in Zusammenhang mit ihrem Träger erneut identifiziert und der Person zugeordnet werden. Für den Betroffenen ist auch nicht abzuschätzen, welche Informationen über ihn aus der Kombination der gerade ausgelesenen Daten, aus der Vergangenheit noch vorgehaltenen sowie unter Abgleich mit statistischen Werten bspw. über so genannte Scoring-Verfahren[458] gewonnen werden können und auch tatsächlich genutzt werden. Wegen dieses Informationsdefizits kann der Betroffene die Einhaltung der für seine Daten geltenden Zweckbindung nur schwer oder gar nicht kontrollieren.

Die Intransparenz der Datenerhebung von Objektnummern einerseits und ihre Verarbeitung in Hintergrundsystemen andererseits eröffnet über ein umfassendes Data Mining „Tür und Tor“ für eine tief in die Privatsphäre des Betroffenen reichende Profilbildung seiner Aufent-

---

[454] Art. 10 GG, § 88 TKG, § 206 StGB; Müller, Jürgen: Ist das Auslesen von RFID-Tags zulässig? – Schutz von RFID-Transponderinformationen durch § 86 TKG, DuD 2004, S. 215, Ohlenburg, Anna, Der neue Telekommunikationsdatenschutz, MMR 2004, S. 431.

[455] § 4 Abs. 1 BDSG.

[456] § 28 Abs. 1 Satz 1 Nr. 2 BDSG reicht als Rechtsgrundlagen nicht aus, weil in diesen Fällen regelmäßig schutzwürdige Interessen des Betroffenen überwiegen. Zusammenfassend Scholz, Datenschutz bei Data Warehousing und Data Mining in: Roßnagel, Handbuch, Kap. 9.2, Rn. 90 ff., 104; Büllesbach, Datenschutz im Konzern, in: Roßnagel, Handbuch, Kap. 7.1., Rn. 36.

[457] Vgl. Petri / Kieper, Datenbevorratungs- und analysesysteme in der Privatwirtschaft, DuD 2003, 609 ff.

[458] Zu den Problemen des Kreditscoring vgl. die Studie des Unabhängigen Landeszentrums für Datenschutz im Auftrag des Bundesministeriums für Verbraucherschutz, http://www.bmelv.de/cln_045/nn_752314/SharedDocs/downloads/02-Verbraucherschutz/Finanzdienstleistungen/scoring.html sowie Möller / Florax, Kreditwirtschaftliche Scoring-Verfahren, MMR 2002, 806.

haltsorte, seines Verhaltens und seiner Interessen, die jenseits der Zweckbindung auf die Erfüllung eines Vertragsverhältnisses für Zwecke der Konsum- oder Freizeitverhaltensanalyse verwendet werden können.[459] Soweit die Beschäftigten am Arbeitsplatz über ihre Objekte erfasst werden, besteht die Möglichkeit einer umfassenden Leistungs- und Verhaltenskontrolle.

Die Betroffenen werden häufig mangels Kenntnis, Zeit oder Kraft überfordert sein, über ihre Datenschutzrechte bspw. auf Auskunft eine Verarbeitung von Objektdaten, die potenziell oder tatsächlich auf ihre Person bezogen sein könnten, zu kontrollieren. Die Aufsichtsbehörden haben zwar mittlerweile die Möglichkeit, auch ohne einen konkreten Anlass die Datenverarbeitung einer verantwortlichen Stelle zu prüfen, die Ressourcen sind aber so beschränkt, dass mit regelmäßigen und flächendeckenden Kontrollen nicht zu rechnen sein wird. Angesichts der Bedeutung und Tiefe der Eingriffe, die sich durch Ubiquitous Computing ergeben können, wird daher über eine Modellierung nachzudenken sein, um Datenschutzverstöße wie bspw. gegen den Zweckbindungsgrundsatz einfacher verfolgen zu können, aber gleichzeitig auch Markteinflüsse zum Schutz des informationellen Selbstbestimmungsrechts wirken zu lassen.[460]

Mit der Verarbeitung von Objekt- und Identifikationsdaten in zentralen Hintergrunddatenbanken stellt sich zudem das Problem der Verantwortlichkeit für die Rechtmäßigkeit der Verarbeitungen. Dies gilt in besonderem Maß, wenn die Hintergrunddatenbanken aus Datenquellen gespeist werden, die von unterschiedlichen Stellen betrieben werden.[461] Unklarheiten über die Verantwortlichkeit für Verarbeitungen innerhalb von UC-Systemen erschweren die Kontrolle und Rechtsdurchsetzung und gehen somit zu Lasten des Betroffenen. Diese Situation kann gegebenenfalls durch eine gesetzliche Neuregelung der Zuweisung von Verantwortung verbessert werden.[462]

Von besonderer Bedeutung ist die Frage, zu welchem Zeitpunkt rechtmäßig für den Zweck des UC-Systems angelegte Benutzerprofile wieder gelöscht werden. Grundsätzlich gilt der datenschutzrechtliche Grundsatz der Erforderlichkeit und der Datensparsamkeit, nach dem personenbezogene Daten zu löschen sind, wenn sie für den angestrebten Zweck nicht mehr benötigt werden.[463] Die Praxis der Speicherung von Log-Files im Internet zeigt, dass Betreiber aus unterschiedlichen Gründen dazu neigen, erlangte Daten im Zweifel länger zu speichern.[464] Sind derartige Daten jedoch erst einmal vorhanden, steigt schnell das Interesse, sie

---

[459] Scholz in: Roßnagel, Handbuch, Kap. 9.2, Rn. 27 ff.; 32.

[460] Siehe unten das Modell zur nutzerzentrierten Gefährdungshaftung.

[461] Siehe oben unter „Outsourcing“ (Kap. 6.2.1.2).

[462] Siehe unten „Verantwortungsräume“ (Kap. 6.3.2) und „nutzerzentrierte Gefährdungshaftung“ (Kap. 6.3.6.2).

[463] § 35 Abs. 2 Satz 1m Satz 2 Nr. 3 BDSG.

[464] Paradigmatisch der Rechtsstreit über die Löschung von IP-Adressen durch den Access-Provider: LG Darmstadt, DuD 2006, 178 ff., aber auch LG Bonn, DuD 2004, 628; dazu Köbele, Anspruch auf Mitteilung, DuD 2004, 609 f. Entsprechendes ist bei den Content-Anbietern im Internet anzunehmen.

auch zu anderen als den ursprünglich angestrebten Zwecken auszuwerten und zu nutzen.[465] Ein Beispiel für diese „Bedarfsweckung" ist die Debatte um die Verwendung der an den Mautbrücken erhobenen Daten, die rechtlich zwar einer strikten Zweckbindung unterliegen, nun aber gleichwohl für Zwecke der Strafverfolgung verwendet werden sollen.[466] Das Beispiel belegt die Bedeutung, technische Lösungen der Datenvermeidung oder Datensparsamkeit in Form von Löschungsroutinen zu implementieren, nachdem der Primärzweck der Daten erreicht worden ist, oder über Pseudonymitätskonzepte die Risiken für die Betroffenen zu minimieren.[467]

6.2.2.4 Adaptive Entscheidungsfindung

Auf der Basis der erhobenen Sensordaten, weiterer Informationen über die Person sowie gegebenenfalls auch statistischer Erkenntnisse findet in dem Hintergrundsystem eine Aufbereitung von Daten statt, auf deren Grundlage das UC-System eine Reaktion gegenüber dem Betroffenen auslöst oder veranlasst. So könnte das Betreten eines Geschäftsraumes durch eine bestimmte Person bspw. eine individualisierte Werbung oder eine persönliche Ansprache mit Namensnennung auslösen. Die Daten können für den Betroffenen aber auch negative Konsequenzen haben, bspw. eine verlängerte Wartezeit, einen höheren Preis für Ware oder Dienstleistung, die Verweigerung eines Vertragsabschlusses oder des Aufenthaltes in den Geschäftsräumen.

Soweit zwischen dem Betroffenen und dem Betreiber ein konkreter Vertrag darüber besteht, dass UC-Leistungen erbracht werden, ist die Verarbeitung nur insoweit zulässig, als sie sich auf die Erfüllung des Vertragsverhältnisses beschränkt.[468] Die Bildung und Nutzung von individualisierten Bewegungs-, Nutzungs- und Kaufprofilen bspw. in einem Supermarkt für Werbezwecke oder zur Optimierung des Verkaufsvorgangs ist von diesem Vertragszweck nicht erfasst.[469] Solche Verarbeitungen bedürfen damit einer informierten und freiwilligen Einwilligung des betroffenen Kunden. Dies erfordert aber auch, dass dem Betroffenen Art, Umfang und Dauer der Verarbeitung der erhobenen Daten sowie ihre konkrete Verwendung verständlich vermittelt wird.

Die Möglichkeit negativer Konsequenzen macht deutlich, dass den erhobenen und verarbeiteten Daten ein Diskriminierungspotenzial inhärent ist. Die Verweigerung eines Vertragsabschlusses liegt letztlich in der Logik der individualisierten Kundenerfassung und -betreuung, bei der nicht nur die zahlungskräftigen Kunden, sondern auch die unzuverlässigeren Interes-

---

[465] Gnirck / Lichtenberg, Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen, DuD 2004, 598 ff.

[466] Zustimmend AG Gummersbach, DuD 2003, 779 f.; ablehnend nun LG Magdeburg; Beschluss vom 3.2.2006, Az.: 25 Qs 7/06, DuD 6/2006; Otten, Zweckbindung im Autobahnmautgesetz, DuD 2006, 657 ff.

[467] Siehe Bizer in: Simitis, BDSG, § 3 a, Rn. 54 ff.; 68 ff.

[468] § 28 Abs. 1 S. 1 Nr. 1 BDSG; Siehe auch Holznagel / Bonnekoh, MMR 2006, 20.

[469] Siehe oben Kap. 6.2.1.4 und Kap. 6.2.2.3.

senten identifiziert werden sollen. Gegenüber dem Prinzip der Abschlussfreiheit, d.h. dass jeder Geschäftsinhaber im Prinzip selbst entscheiden kann, ob er mit einem potenziellen Kunden einen Vertrag abschließen will, gewinnt die Datenerfassung und –verarbeitung im Vorfeld der Vertragsanbahnung eine neue Qualität. Entsprechendes gilt auch für die Möglichkeit zur sozialen oder politischen Kommunikation. Die Daten in dem Hintergrundsystem ermöglichen letztlich eine Vorauswahl derjenigen, denen eine Chance auf einen sozialen Kontakt oder einen Vertragsabschluss eröffnet werden soll.

Wird über eine UC-Anwendung der Zutritt zu der Öffentlichkeit zugänglichen Räumen oder Flächen wie z.B. Einkaufspassagen, Bahnhöfen oder öffentlichen Verkehrsflächen u.ä. gesteuert, dann wirkt sich eine positive wie negative Auswahlsteuerung unmittelbar auf die Möglichkeiten zur sozialen und auch politischen Kommunikation aus. Bei öffentlichen Verkehrsflächen, die wie z.B. Fußgängerzonen oder Plätze auch dem „kommunikativen Gemeingebrauch“ [470] gewidmet sind, wäre eine solche Auswahlsteuerung unzulässig, weil sie die Chancen zur sozialen Kommunikation ohne einen sachlichen Grund beschränken würde.[471] Problematisch wäre aber auch eine Auswahlsteuerung zu öffentlich zugänglichen, aber in privatem Besitz betriebenen Räumen wie Einkaufspassagen oder Verkehrsflächen. Zutritt und Aufenthalt kann von dem Eigentümer regelmäßig auf der Grundlage seines Hausrechts festgelegt werden. Öffentliche Räume sind aber gleichwohl für die soziale Kommunikation nicht ohne Bedeutung, so dass eine Auswahlsteuerung auch hier nicht ohne einen sachlichen Grund wie eine Abwehr konkreter Störungen oder Gefahren erfolgen darf. Unter diesem Gesichtspunkt ist für den Betroffenen nicht nur von Bedeutung, welche Daten im Hintergrundsystem über ihn gesammelt werden, sondern auch welche Faktoren der Algorithmus des Systems für seine Bewertungen und Entscheidungen zugrunde legt. Rechtlich ist die Situation insofern nicht wesentlich anders als die eines Scoringsystems zu bewerten, das ein zukünftiges Verhalten auf der Grundlage von individuellen Erfahrungswerten und statistischen Größen zu prognostizieren versucht und dessen Funktionsweise gegenüber dem Betroffenen offen gelegt werden muss.[472]

Schließlich ist zu beachten, dass neben dem europarechtlichen Verbot der Diskriminierung[473] für die Verarbeitung und damit auch Auswertung personenbezogener Daten besondere Voraussetzungen gelten, wenn es sich um so genannte „besondere Datenarten“ nach § 3 Abs. 9 BDSG handelt. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Im Regelfall ist eine Verarbeitung dieser Daten nur mit

---

[470] VGH Baden-Württemberg, VBlBW 1997, 64.

[471] Sachliche Gründe waren Tatbestände, die eine Sondernutzungserlaubnis erforderlich machen. Hierzu gehört bspw. das Musizieren oder das Aufstellen eines Büchertisches in einer Fußgängerzone.

[472] ULD, Gutachten Scoringsysteme; Weichert, DuD 2005, 582 ff.

[473] Siehe Die EG-Antidiskrimierungsrichtlinie 2000/43/EG vom 29. Juni 2000 enthält insbesondere ein Diskriminierungsverbot für den Zugang zu „Gütern und Dienstleistungen“. Die Gesetzgebung zur Umsetzung dieser Richtlinie ist in der letzten Legislaturperiode stecken geblieben, Gesetzentwurf zur Umsetzung europäischer Antidiskriminierungsrichtlinien, BT-Drs. 15/4538 vom 16.12.2004.

Einwilligung des Betroffenen zulässig.[474]

6.2.2.5 Automatisierte Maßnahmen

Auf der Grundlage der oben beschriebenen Maßnahmen zur adaptiven Entscheidungsfindung lösen UC-Systeme aufgrund von erfassten Informationen bestimmte Handlungen aus. Beispiele sind, dass in einem Ladengeschäft ein Kunde automatisch erkannt, begrüßt oder abgewiesen wird, dass in einem Zimmer der Anwesende automatisch erkannt, seine Bedürfnisse bzgl. Klima und Raumtemperatur identifiziert und die Umgebungsbedingungen entsprechend reguliert werden oder dass in einem Kraftfahrzeug die Komforteinstellungen wie Sitzhöhe und Rückspiegel insassenspezifisch automatisch erfolgen. In UC-Anwendungen werden also auf der Basis automatisierter Auswertungen personenbezogener Daten Entscheidungen vorbereitet und getroffen, die sich unmittelbar auf die Personen auswirken.

Nach § 6 a Abs. 1 BDSG darf eine Entscheidung nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Mit dieser Regelung, die auf Art. 15 der EG-Datenschutzrichtlinie zurückgeht, soll der Betroffene davor geschützt werden, dass nur noch maschinell erzeugte Entscheidungen aufgrund eines automatisierten Persönlichkeitsprofils erstellt werden, ohne dass eine Person den Sachverhalt neu überprüft.[475] Voraussetzung für das Verbot automatisierter Entscheidungen ist, dass sie den Betroffenen „erheblich beeinträchtigt“ oder für den Betroffenen „eine rechtliche Folge nach sich zieht“.[476] Letzteres ist bereits dann der Fall, wenn sich aus der automatisierten Entscheidung ein Rechtsverhältnis wie bspw. ein Vertragsverhältnis ergibt, aus dem sich Ansprüche auf ein Handeln oder Unterlassen ergeben.[477] Eine solche rechtliche Folge könnte von einem UC-System wie bspw. einem selbstständig nachbestellenden Kühlschrank ausgelöst werden, der für seinen Besitzer selbständig Vertragsverhältnisse mit Lebensmittellieferanten abschließt und ihn zur Abnahme sowie zur Zahlung verpflichtet. Erhebliche Beeinträchtigungen könnten sich insbesondere aus fehlerhaften Bestellungen oder Lieferungen ergeben, die die Gesundheit der Nutzer des Kühlschrankes beeinträchtigen.

Die Verarbeitungen dürfen nicht der Bewertung einzelner Persönlichkeitsmerkmale dienen. Gemeint sind damit Daten, die die Persönlichkeit des Betroffenen unter bestimmten „einzelnen Aspekten“ beschreiben (z.B. die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit oder das Verhalten einer Person).[478] Dies schließt eine Vielzahl von Scoring-, Data Mining- und Profiling-Techniken aus, auf die sich über eine adaptive Entscheidungsfindung die automatisierte Ausführung einzelner Handlungen stützen. Eine automatisierte Prüfung der Kreditwürdigkeit oder eines bestimmten Arbeitsverhaltens ist unzulässiger Bestand-

[474] Siehe näher §§ 28 Abs. 6 ff. BDSG.

[475] Bizer in: Simitis, § 6 a, Rn. 3.

[476] So § 6 a Abs. 1, 1. Alternative BDSG.

[477] Bizer in: Simitis, BDSG, § 6 a, Rn. 16 ff.

[478] Bizer in: Simitis, BDSG, § 6 a, Rn. 30 ff.; Gola / Schomerus, BDSG, § 6 a, Rn. 7.

teil eines UC-Systems, wenn sich an die Prüfung ein systemgesteuertes Handeln im Sinne einer Entscheidung knüpft.[479] Das Verbot automatisierter Entscheidung nach § 6 a BDSG wäre erst dann nicht einschlägig, wenn der Ausgang der Entscheidung im Einzelfall noch von einer Person beeinflusst werden würde.[480] Im Regelfall sollen UC-Systeme aus Komfort- oder Kostengründen eine Letztentscheidung durch einen Menschen aber gerade ausschließen. Aus demselben Grund wird für UC-Anwendungen auch die Ausnahme des § 6 a Abs. 2 Nr. 2 BDSG keine praktische Bedeutung haben, wonach automatisierte Entscheidungen nicht verboten sind, wenn dem Betroffenen die Tatsache einer solchen Entscheidung mitgeteilt wird, er die Möglichkeit bekommt, seinen Standpunkt dazulegen und eine erneute Prüfung der Entscheidung durch die verantwortliche Stelle erfolgt.[481] Das Verbot automatisierter Einzelentscheidungen ist also für UC-Systeme regelmäßig von Bedeutung und zu beachten.

Ausgenommen sind von dem Verbot der automatisierten Entscheidung nur folgende Konstellationen. Nach § 6 a Abs. 2 Nr. 1 BDSG gilt das Verbot nicht, wenn die Entscheidung im Rahmen oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht „und dem Begehren des Betroffenen stattgegeben wurde“. Dieses wäre bspw. der Fall, wenn im oben genannten Kühlschrankbeispiel mit der Lieferung der Ware ein Vertrag über die Nachlieferung von Waren erfüllt werden würde. Erfüllt die automatisierte Entscheidung also eine vertragliche Verpflichtung gegenüber dem Betroffenen auf seinen Wunsch, so dass sie für ihn keine Nachteile bereitet, dann ist eine automatisierte Entscheidung nach § 6 a BDSG nicht verboten. Dasselbe gilt auch dann, wenn durch die automatisierte Entscheidung ein Vertragsangebot des Betroffenen von der Gegenseite angenommen wird.[482]

Automatisierte Entscheidungen sind in UC-Systemen demnach nicht verboten, wenn sie das Begehren im Rahmen des Abschlusses oder der Erfüllung eines Vertrags- oder eines sonstigen Rechtsverhältnisses erfüllen. Sie sind aber in den Fällen untersagt, in denen die Entscheidung eine negative Auswirkung auf den Betroffenen hat. Dies kann der Fall sein, wenn ein Begehren des Betroffenen abgelehnt wird, aber auch wenn im Vorfeld von Entscheidungen eine Auswahlentscheidung zwischen Personen nach Persönlichkeitskriterien getroffen wird.

6.3 Rechtliche Möglichkeiten zur Minimierung der Risiken

6.3.1 Regelungsansätze

Das Regelungsziel des Datenschutzes wird über eine Mischung von Instrumenten und Me-

[479] Das Verbot automatisierter Entscheidung nach § 6 a BDSG ergänzt also das Verbot der automatisierten Auswertung und Generierung von Profildaten ohne Mitwirkung des Betroffenen (s. Kap. 6.2.2.4).

[480] Bizer in: Simitis, BDSG, § 6 a, Rn. 27 f.

[481] Näher Bizer in: Simitis, BDSG, § 6 a, Rn. 42 ff.

[482] Bizer in: Simitis, BDSG, § 6 a, Rn. 40 f.

thoden durchgesetzt. Im Vordergrund steht das am klassischen Ordnungsrecht orientierte Verbot jeder Verarbeitung personenbezogener Daten, das unter dem Vorbehalt einer ausdrücklichen Erlaubnis aufgrund eines gesetzlichen Tatbestandes oder einer informierten und freiwilligen Einwilligung des Betroffenen steht („Datenschutzrechtlicher Erlaubnisvorbehalt").[483] Dieser Ansatz wird flankiert durch eine Reihe von weiteren Vorgaben wie der Zweckbindung, der Erforderlichkeit sowie der Transparenz der Datenverarbeitung, deren Befolgung durch interne Institutionen wie den betrieblichen Datenschutzbeauftragten sowie durch externe Stellen wie die Aufsichtsbehörden kontrolliert werden. Dieses Steuerungsmodell des Datenschutzrechts muss auf die Herausforderungen des Ubiquitous Computing überprüft und gegebenenfalls auch angepasst werden (s.u. Kap. 6.3.3).

Datenschutz dient der Sicherung der informationellen Selbstbestimmung. Diese schützt wiederum die Befugnis des Einzelnen, „grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen".[484] Dem Schutzgehalt der informationellen Selbstbestimmung entspricht es folglich, wenn der Betroffene in erster Linie selbst die Möglichkeit hat, einer Verwendung seiner Daten zuzustimmen oder sie zu verweigern. In der Datenschutzliteratur wird dies auch als *Selbstdatenschutz* bezeichnet.[485] In einem umfassenderen Sinne werden unter Selbstdatenschutz die Rechte des Betroffenen, aber auch die technischen Schutzmechanismen verstanden, mit denen er seine Daten selbst schützen kann. Zu prüfen ist, durch welche Maßnahmen die Rechte der Betroffenen zum Selbstdatenschutz in UC-Anwendungen gestärkt und umgesetzt werden können (s.u. Kap. 6.3.4).

Datenschutzprobleme entstehen u.a. aus der Verarbeitung personenbezogener Daten in technischen Systemen, die für bestimmte Zwecke gestaltet und eingesetzt werden. Solche Risiken für die informationelle Selbstbestimmung lassen sich erfahrungsgemäß allein durch Mittel des Datenschutzrechts nur ungenügend vermeiden oder begrenzen. Die wesentlichen Gründe sind, dass auf einen Verstoß gegen eine Rechtsregel nur reaktiv Konsequenzen folgen können, die auf eine nachträgliche Änderung der Datenverarbeitung zielen. In diesem Fall ist der Eingriff in das informationelle Selbstbestimmungsrecht aber schon erfolgt. Gleichzeitig sind die Ressourcen der staatlichen Datenschutzkontrolle beschränkt, so dass die Verarbeitung personenbezogener Daten insbesondere in komplexeren technischen Umfeldern nicht wirksam kontrolliert werden kann. Im Interesse der Betroffenen erfordert ein effektiver Datenschutz daher eine proaktive Vermeidungsstrategie, die Verstöße gegen den Datenschutz bereits im Vorfeld vermeidet.

Um dies zu erreichen, wird im modernen Datenschutz das klassische Schutzkonzept des Datenschutzrechts durch einen proaktiven Ansatz ergänzt und erweitert, den „*Datenschutz*

[483] Zusammenfassende Skizze bei Bizer, Datenschutzrecht in: Schulte, Handbuch des Technikrechts, Heidelberg 2003, S. 581 ff.

[484] BVerfGE 65, 1 , 42.

[485] Siehe Roßnagel, Konzepte des Selbstdatenschutzes in: ders., Handbuch des Datenschutzrechts, Kap. 3.4; Bizer, Datenschutzrecht in: Schulte, Handbuch des Technikrechts, S. 591 f. m.w.N.

durch Technik" in die Produkte und Datenverarbeitungssysteme zu implementieren.[486] Ein solches Konzept wirkt in einem doppelten Sinne vorbeugend: Der Datenschutz soll proaktiv wirken und muss daher bereits bei der technischen Gestaltung der Systeme berücksichtigt werden. Paradigmatisch ist in dieser Hinsicht § 3 a BDSG, mit dem der Gesetzgeber für das Konzept der datenvermeidenden und datensparsamen Technikgestaltung und Auswahl eine normative Grundlage vorgegeben hat. Darüber hinaus bedeutet „Datenschutz durch Technik" aber auch, dem Betroffenen Mittel an die Hand zu geben, mit denen er seine informationelle Selbstbestimmung ausüben und seine Daten wirksam schützen kann.[487] Es ist also zu prüfen, durch welche technischen und organisatorischen Maßnahmen die Betroffenenrechte in UC-Anwendungen gewahrt und gestärkt werden können (s.u. Kap. 6.3.5).

Den größten Wirkungsgrad erzielen Regelungen, die von den Normadressaten aus eigener Motivation umgesetzt werden. Aus diesem Grund erhalten ökonomische Instrumente für die Umsetzung der datenschutzrechtlichen Anforderungen eine immer größere Bedeutung, um im Interesse der Betroffenen und der verarbeitenden Stellen positive Wirkungen zu Gunsten von Datenschutz und Datensicherheit zu erzeugen.[488] Erreicht wird dies durch das Angebot freiwilliger Zertifizierungen, die für datenschutzkonforme Produkte und Dienstleistungen von einer unabhängigen und von den Verbrauchern anerkannten Stelle vergeben werden. Solche Instrumente zielen auf das wirtschaftliche Interesse der verantwortlichen Stellen, im Interesse ihrer Kunden und damit im wohlverstandenen eigenen wirtschaftlichen Interesse Produkte und Dienstleistungen datenschutzkonform zu gestalten. Das Zertifikat belohnt diesen Erfolg, indem es Investitionen in den Datenschutz durch die Verleihung eines im Wettbewerb wirksamen Gütesiegels unterstützt.

Mit § 9 a BDSG hat der Bundesgesetzgeber eine allgemeine Rahmenbestimmung für diese beiden Instrumente geschaffen.[489] Ein prominentes Beispiel ist das Datenschutz-Gütesiegel aus Schleswig-Holstein, das von dem Unabhängigen Landeszentrum für Datenschutz seit Bestehen über 30 Mal an Hersteller für die datenschutzfreundliche Gestaltung eines Produktes verliehen worden ist.[490] Ein zweites Instrument ist das Datenschutz-Audit, das in Schleswig-Holstein für die datenschutzkonforme Gestaltung von automatisierten Verfahren der Da-

[486] Vgl. Bizer, Datenschutz durch Technikgestaltung in: Bäumler / v. Mutius, Datenschutzgesetze der dritten Generation, Neuwied 1999, S. 28 ff., 45 ff. Bizer in: Simitis, BDSG, § 3 a, Rn. 10 ff. m.w.N.

[487] Hansen, Privacy Enhancing Technologies in: Roßnagel, Handbuch des Datenschutzrecht, Kap. 3.3, Rn. 76 ff.; Roßnagel, Konzepte des Selbstdatenschutzes in: ders., Handbuch des Datenschutzrechts, Kap. 3.4, Rn. 44 ff.

[488] Siehe Bäumler / von Mutius, Datenschutz als Wettbewerbsvorteil; Roßnagel, Datenschutzaudit in: ders., Handbuch des Datenschutzrechts, Kap. 3.7.; Büllesbach, Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor, RDV 1997, 239 ff.

[489] Siehe Bizer in: Simitis, BDSG, § 9 a.

[490] Bizer / Körffer, Gütesiegel für IT-Produkte, WuM 2006, 24 ff.; Bäumler, Marktwirtschaftlicher Datenschutz, DuD 2002, 325 ff.; Schläger, Gütesiegel nach Datenschutzauditverordnung Schleswig-Holstein, DuD 2004, 459 ff.

tenverarbeitung in Behörden verliehen wird.[491] Auch in der Wirtschaft hat die Zertifizierung von Verfahren nach anerkannten Maßstäben und damit auch die von Datenschutz und Datensicherheit Bedeutung, um den von einer Organisation erreichten Zustand an den vorgegebenen Zielen messen zu können.[492] Auch diese ökonomischen Instrumente gilt es für die Datenschutzkontrolle des Ubiquitous Computing fruchtbar zu machen (s.u. Kap. 6.3.6).

6.3.2 Verantwortungsräume

Regulatorischer Anknüpfungspunkt für Rechte und Pflichten im Datenschutz ist die Stelle, „die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“ (§ 3 Abs. 7 BDSG). Diese Stelle ist – um einige Beispiele zu nennen – verpflichtet, die Verwendungszwecke der Daten bei der Erhebung festzulegen (§ 28 Abs. 1 Satz 2 BDSG), die Betroffenen über ihre Identität, die Verwendungszwecke sowie die (Kategorien der) Empfänger zu unterrichten (§ 4 Abs. 3 BDSG) und im Fall einer Auftragsdatenverarbeitung, den Auftragnehmern Weisungen zu erteilen und ihre Einhaltung zu überwachen.

Für die Datenerhebung und –verarbeitung verantwortliche Stelle in UC-Systemen ist der Betreiber des Hintergrundsystems, das die Datenerhebung über die Sensoren und Lesegeräte steuert und zu einem bestimmten Zweck verarbeitet. Ein Beispiel für eine solche UC-Anwendung ist der Betreiber eines UC-Hauses, in dem die Funktionen des Hauses wie die Raumtemperatur, die Beleuchtung, die Musik u.a. Umgebungsbedingungen personenabhängig gesteuert werden. Ein anderes Beispiel ist das UC-Kraftfahrzeug, in dem die Einstellung der Parameter des Autos automatisiert in Abhängigkeit vom Fahrer bzw. Mitfahrer vorgenommen wird. Ein letztes Beispiel ist das Geschäft in der Einkaufsmeile, das seine Besucher bereits vor der Schaufensterscheibe erkennt und mit kundenspezifischen werblichen Hinweisen anspricht. Die Sensoren erfassen bspw. die Objektnummern aus bestimmten RFID-Tags, lesen sie aus und übermitteln sie an ein Hintergrundssystem, das die Person des Trägers über die Zuordnung von Objektnummer zu den Identifizierungsdaten erkennt. Für den Regelfall einer Datenerhebung ist daher davon auszugehen, dass der Betreiber des Hintergrundsystems die für Datenverarbeitung verantwortliche Stelle ist und damit auch gegenüber dem Betroffenen für die Rechtmäßigkeit der Verarbeitung die Verantwortung trägt.

Grundsätzlich kann davon ausgegangen werden, dass Lesegeräte bzw. Sensoren weder absichtslos noch ohne Verwendungszweck aufgestellt und betrieben werden. Vielmehr werden die für die Beschaffung und den Betrieb erforderlichen Investitionen sich durch die verfolgten Ziele betriebswirtschaftlich rechtfertigen lassen müssen. Um ihre Aufgabe einer ge-

[491] Bäumler / von Mutius, Datenschutz als Wettbewerbsvorteil; Behrendt, Datenschutzaudit in der Praxis, DuD 2006, 20 ff.

[492] Vgl. Bizer, Bausteine des Datenschutzaudits, DuD 2006, 5 ff.; Meints, Datenschutz nach BSI-Grundschutz, DuD 2006, 13 ff.; Zwick, Standardisierung im Datenschutz, DuD 2006, 26 ff.; Reiländer / Weck, Datenschutzaudit nach IT-Grundschutz – Konvergenz zweier Welten, DuD 2003, 692 ff.

zielten Erfassung von Objekten und gegebenenfalls auch eine Zuordnung zu ihren jeweiligen Trägern erfüllen zu können, werden Lesegeräte bzw. Sensoren regelmäßig funktions- und damit raumbezogen aufgestellt sowie über ein Hintergrundsystem miteinander verbunden. Dass Lesegeräte bzw. Sensoren ohne einen konkreten Verwendungszweck aufgestellt und ohne Verknüpfung zu einem Hintergrundsystem betrieben werden, ist zwar nicht auszuschließen, aber ökonomisch wenig sinnvoll und kann daher zunächst vernachlässigt werden.

UC-Systeme werden, um ihre jeweiligen Beschaffungs- und Betriebskosten zu decken, regelmäßig von denjenigen installiert und betrieben werden, die in oder vor Geschäften oder öffentlichen Einrichtungen Objekte bzw. Personen identifizieren wollen. Entsprechendes gilt für Anwendungen wie das UC-Kraftfahrzeug oder das UC-Haus. Derartigen Anwendungen ist gemeinsam, dass die Einrichtungen des UC-Systems von einem Betreiber aufgestellt und betrieben werden, der für einen bestimmten Funktionsraum ein spezifisches Betriebsinteresse der Datenerfassung verfolgt. So vielfältig die Möglichkeiten des Auslesens von Objektdaten in solchen Räumen auch immer sein werden, verantwortlich für die Erhebung wird immer der jeweilige Betreiber sein, der die technischen Einrichtungen der Datenerfassung wie Lesegeräte und Sensoren über ein Hintergrundsystem verbindet, Objektdaten erfasst und verarbeitet sowie über die Möglichkeit einer Verknüpfung mit den Trägern der Objekte verfügt. Sollten Lesegeräte bzw. Sensoren zwei oder mehrere Hintergrundsysteme unterschiedlicher Betreiber mit Daten versorgen, so ist jeder Betreiber seines Systems insoweit auch für die Erhebung und weitere Verarbeitung der Daten verantwortlich und muss damit für die Rechtmäßigkeit seiner Datenerhebung und -verarbeitung einstehen. Erfolgt die Datenverarbeitung auf den Chips der Datenobjekte, so ist in Anlehnung an § 6 c Abs. 1 BDSG diejenige Stelle verantwortlich, die das Speichermedium über das Trägerobjekt ausgegeben oder das Medium programmiert hat.

Die Erhebung personenbeziehbarer Daten über UC-Systeme ist wie jede heimliche Datenerfassung für die Betroffenen intransparent, sie erfolgt aber datenschutzrechtlich nicht bindungslos. Das klassische Datenschutzrecht verfügt mit dem Prinzip der Verantwortlichkeit der Datenverarbeitung über ein leistungsfähiges Instrument, das für UC-Systeme mit der Verantwortung für die Datenerhebung in spezifischen Anwendungsräumen konkretisiert werden kann. Von der für das Hintergrundsystem verantwortlichen Stelle aus betrachtet ist diese für UC-Erhebungen in den Räumen verantwortlich, in denen sie über Lesegeräte bzw. Sensoren Objekt- und Umgebungsdaten erhebt. Dabei ist für die Rechtmäßigkeit der Erhebung nicht maßgeblich, ob der Betreiber des Hintergrundsystems diese selbst betreibt oder die erhobenen Daten lediglich verwendet. In jedem Fall wird sich der Betreiber des Hintergrundsystems die Datenerhebungen zurechnen lassen müssen, die er in seinem System verarbeitet.[493]

Soweit die Einrichtungen des Auslesens (Lesegeräten bzw. Sensoren) ortsfest installiert werden, wird dies regelmäßig nur auf Veranlassung oder mit Zustimmung des Inhabers des

[493] Etwas anderes wäre anzunehmen, wenn die Daten aus einem Hintergrundsystem an einen Dritten übermittelt werden. In diesem Fall betreibt der Dritte aber kein Hintergrundsystem, sondern bedient sich einer anderen Stelle als Datenquelle.

Hausrechts erfolgen. Der Inhaber des Hausrechts trägt mit anderen Worten ebenfalls eine rechtliche Verantwortung gegenüber den Betroffenen, dass eine personenbeziehbare Erfassung ihrer Objektdaten in seinen Räumlichkeiten erfolgt. Soweit der Inhaber des Hausrechts auch die Verantwortung für das Hintergrundsystem trägt, liegt diese in einer Hand. Im anderen Fall besteht die Verantwortung des Hausrechtsinhabers unabhängig von dem Betreiber des Hintergrundsystems, wenn er die Aufstellung von Lesegeräten bzw. Sensoren vornehmen lässt oder duldet. Sie folgt aus der Verpflichtung des Hausherren - sei es aus vertraglicher Nebenpflicht oder aus deliktsrechtlichen Verkehrssicherungspflichten -, die Rechtsgüter seiner Besucher zu schützen. Der betroffene Besucher hat gegenüber dem Inhaber des Hausrechts einen Anspruch, dass dieser Störungen seiner Privatsphäre unterlässt.[494]

Eine rechtliche Verantwortung für das Auslesen über mobile Lesegeräte bzw. Sensoren trägt der Inhaber des Hausrechts, wenn er diese veranlasst hat bzw. in seinen Räumlichkeiten duldet. Im Übrigen kann der Inhaber des Hausrechts nur zu einem ihm möglichen Verhalten verpflichtet sein. Ist der Betrieb mobiler Lesegeräte bzw. Sensoren durch Dritte von dem Inhaber des Hausrechts nicht festzustellen, weil sie bspw. nicht über eine entsprechende Signalisierung verfügen, dann kann er seine Besucher vor einer entsprechenden Erfassung auch nicht wirksam schützen. Ließe sich mit einem vertretbaren Aufwand der Betrieb solcher Einrichtungen feststellen, dann wäre eine entsprechende Fortentwicklung der Verkehrssicherungspflichten zum Schutz der Besucher voranzutreiben. In jedem Fall bleibt es bei der rechtlichen Verantwortung des Betreibers für die Zusammenführung und Verarbeitung von personenbeziehbaren Objektdaten und Identifizierungsdaten in dem jeweiligen Hintergrundsystem.

6.3.3 Direkt steuernde Maßnahmen

Ein Grundproblem der Anwendung von UC-Systemen mit nationaler wie internationaler personenbezogener Datenverarbeitung ist die Rechtsdurchsetzung. Wenn das bisher durch die EG-Datenschutzrichtlinie vorgesehene und im BDSG bzw. den LDSG der Länder vorgesehene Modell der Datenschutzbeauftragten bzw. der Datenschutzaufsichtsbehörden wirksam kontrollierend Einfluss auf die personenbezogene Datenverarbeitung im UC nehmen soll, wird eine engere inhaltliche Koordination und Abstimmung zwischen diesen Stellen auf nationaler wie internationaler Ebene erforderlich sein.

Ein für UC spezifischer Umstand ist, dass die Qualifizierung der über Lesegeräte bzw. Sensorik erhobenen Daten als personenbezogen im Regelfall erst mit Kenntnis der Verarbeitungsvorgänge in für den Betroffenen nicht transparenten Hintergrundsystemen möglich ist.[495] Die Anwendung der Datenschutzvorschriften darf aber nicht zu unterschiedlichen

[494] So genannter „Störerabwehranspruch“ aus § 1004 BGB analog bzw. auch § 823 i.V.m. § 1004 BGB.

[495] Siehe die Diskussion in der Art. 29 Gruppe: Ergebnisse der öffentlichen Anhörung zum Arbeitspapier 105 der Art. 29 Arbeitsgruppe zum Thema Datenschutz und RFID-Technologie, http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_de.pdf

Schutzstandards führen, nur weil Verarbeitungsvorgänge in Hintergrundsystemen nicht bekannt, nachweisbar oder kontrollierbar (z.B. da im Ausland stattfindend) sind. Dieser Unsicherheit könnte eine von der verantwortlichen Stelle zu widerlegende Vermutung der Personenbeziehbarkeit der in einem UC-System über Lesegeräte bzw. Sensoren erfassten Daten entgegenwirken. Nach einer solchen Regel wären die von UC-Systemen erfassten Daten grundsätzlich als personenbezogen zu bewerten und damit Datenschutzrecht anzuwenden. Die für die Erhebung verantwortliche Stelle hätte aber die Möglichkeit, diese Vermutung zu widerlegen. Eine solche Auslegungsregel ist interessengerecht, weil die für die Erhebung und Verarbeitung verantwortliche Stelle im Unterschied zu den Betroffenen die Struktur und Verarbeitungsvorgänge des UC-Systems kennt und für seine Steuerung verantwortlich ist. Gleichzeitig würde eine solche Regel die Kontrollmöglichkeit der Verarbeitung in der Praxis deutlich stärken. Dies gilt nicht nur für im Binnenmarkt betriebene UC-Systeme, sondern insbesondere auch für die Auslagerung von Verarbeitungen in so genannte „unsichere Drittstaaten“, mit denen nationale und europäische Vorgaben im Wege eines „Datenschutz-Shopping“ unterlaufen werden können.

Zur Risikominimierung bei riskanten Datenverarbeitungen stellt das Datenschutzrecht das Instrument der Vorabkontrolle bereit.[496] Mit diesem Instrument hat der betriebliche Datenschutzbeauftragte solche Verarbeitungen im Wege einer präventiven Rechtmäßigkeitskontrolle zu prüfen, bevor sie in Betrieb gehen. Aufgrund ihrer systemimmanenten Komplexität und des damit gesteigerten Risikos für das informationelle Selbstbestimmungsrecht wird auch für UC-Systeme grundsätzlich eine Vorabkontrolle durchzuführen sein. Auf diese Weise können datenschutzrechtliche Fragen - von der Rechtmäßigkeit bis zur Gestaltung der gegenüber den Betroffenen erforderlichen Transparenz - innerbetrieblich geklärt und die Erhebung und Verarbeitung personenbeziehbarer Daten rechtskonform vor ihrer Betriebsaufnahme geklärt werden. Aus der Vorabkontrolle geht auch die Verpflichtung des Betreibers von UC-Systemen einher, einen betrieblichen Datenschutzbeauftragten unabhängig von der Anzahl der mit personenbezogener Datenverarbeitung befassten Mitarbeiter zu bestellen, der fachlich qualifiziert ist, eine solche Vorabkontrolle durchzuführen.

Zur Lösung des Transparenzproblems und zu Gunsten des von einer Verarbeitung in einem UC-System Betroffenen ist es erforderlich, dem Betreiber eines Hintergrundsystems weitergehende Informationspflichten aufzuerlegen.[497] Spiegelbildlich muss der Betroffene diese Informationen auch im Wege eines Auskunftsanspruches erhalten können. Die zusätzlichen

[496] § 4 d Abs. 5 und 6 BDSG.

[497] Nach § 4 Abs. 3 BDSG muss die verantwortliche Stelle den Betroffenen unterrichten (1.) über ihre Identität, (2.) die Zweckbestimmungen der Erhebungen, Verarbeitungen oder Nutzungen und (3.) die Kategorien von Empfängern, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.
Nach § 6 c Abs. 1 BDSG hat die Stelle, die mobile personenbezogene Speicher- und Verarbeitungsmedien bspw. ausgibt, den Betroffenen zu unterrichten über (1.) ihre Identität und Anschrift, (2.) in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten, (3.) darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und (4.) über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen.

Informationen müssen die Art, Herkunft und Zweckbindung der Daten umfassen, die zu Kombinationszwecken verwendet werden. Der Betroffene muss ferner unterrichtet werden über die logische Struktur der Kombinationen und Auswertungen, die einzelnen Kriterien sowie die erfassten Datenkategorien.[498] Diese Informationen sind notwendig, um dem Betroffenen eine eigenständige und gegebenenfalls mit entsprechender Unterstützung unabhängige Beurteilung zu ermöglichen, ob und welche Verarbeitungen im Hintergrundsystem rechtmäßig erfolgen. Die Informationen würden gleichzeitig eine zügige Fremdkontrolle durch die jeweils zuständige Aufsichtsbehörde unterstützen, in dem sie den Aufwand für die Sachverhaltsermittlung weitgehend auf Stichproben der Nachvollziehbarkeit reduziert.

Eine besondere Herausforderung stellt die Vermittlung der datenschutzrechtlich gebotenen Informationen an die Betroffenen dar.[499] Die Informationen müssen so verständlich aufbereitet sein, dass sie dem Betroffenen Art, Umfang und Bedeutung der Datenverarbeitung vermitteln. Sie müssen den Betroffenen vor allem auch tatsächlich erreichen und für ihn dauerhaft verfügbar sein. Soweit Daten der Betroffenen über UC-Systeme im Rahmen eines Vertragsverhältnisses erfasst und verarbeitet werden, können die Betroffenen bei Vertragsschluss in geeigneter Form unterrichtet werden.[500] Schwieriger stellt sich die Information der Betroffenen bei einer Erhebung in Anwendungsräumen dar, ohne dass eine ausdrückliche und formalisierte vertragliche Beziehung besteht. In diesen Fällen bedarf es zumindest einer optischen Unterrichtung der Betroffenen im Wege eines selbsterklärenden und einheitlichen Symbols, dass durch Lesegeräte bzw. Sensoren Objektdaten erfasst und ausgelesen werden. Die Symbole bedürfen darüber hinaus eines Hinweises auf die für die Erhebung verantwortliche Stelle.[501] Verantwortlich für diese Hinweise sind in öffentlich zugänglichen Räumen der Inhaber des Hausrechts sowie der Betreiber des Hintergrundsystems, in dem die erfassten Daten zusammengeführt werden.

Die Kommunikation in UC-Systemen zwischen Lesegeräten bzw. Sensoren und Hintergrundsystem wird häufig auf Telekommunikation beruhen. Informationen, die den an dem Betrieb des UC-Systems Beteiligten über diese Kommunikationen bekannt werden, unterliegen dem Telekommunikationsgeheimnis, soweit diese Übertragungsdienste geschäftsmäßig angeboten werden.[502] Dieser rechtliche Schutz würde jedoch entfallen, wenn für das UC-

[498] Ein erster Ansatz für eine solche Regelung findet sich im Verbot automatisierter Einzelentscheidungen nach § 6 a Abs. 3 BDSG. Danach erstreckt sich das Auskunftsrecht auch auf den „logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten".

[499] Sowohl § 6 c Abs. 1 Nr. 2 BDSG als auch § 291 a Abs. 3 Satz 3 SGB V (Elektronische Gesundheitskarte) fordern eine Unterrichtung in „allgemein verständlicher Form".

[500] Eine solche Regelung gilt nach dem Fernabsatzrecht. Nach § 313 c Abs. 1, 2 BGB hat der Unternehmer dem Verbraucher bestimmte Informationen vor bzw. bei Vertragsschluss zur Verfügung zu stellen.

[501] Eine Parallele findet sich für die Videoüberwachung öffentlicher Räume, für die in § 6 b Abs. 2 BDSG vorgeschrieben ist, dass der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen ist. Ein solches Symbol ist als Piktogramm bspw. in DIN 33450 normiert.

[502] § 88 Abs. 2 i.Vm. § 3 Nr. 6 TKG.

System technisch-organisatorische Konfigurationen verwendet werden, die außerhalb des Anwendungsbereichs des Fernmeldegeheimnisses liegen. Zur Absicherung des Datenaustausches sowie zur Rechtsklarheit für UC-Betreiber und Nutzer sollte der Schutzstandard des Telekommunikationsgeheimnisses für jede Datenübertragung in UC-Systemen gelten. Auf diese Weise könnte im Übrigen auch das Vertrauen der Nutzer in die Sicherheit der Datenübertragung in UC-Systemen gestärkt werden.

Um einer heimlichen und unbefugten Identifizierung von Personen mit Hilfe von RFID-Lesegeräten abschreckend vorzubeugen, sollte das entsprechende datenschutzrechtliche Verbot durch eine deutliche Strafbewehrung sanktioniert werden.

6.3.4 Maßnahmen zur Unterstützung des Betroffenen

Der Einsatz von UC-Diensten im Alltag wird die Zahl der Datenverarbeiter sowie der personenbezogenen Datenverarbeitungen deutlich ansteigen lassen. Diese Tatsache und eine erhöhte Komplexität der Verarbeitung durch die damit verbundene Vernetzung wird die staatliche Datenschutzkontrolle vor ein erhebliches Massenproblem stellen, das letztlich nur durch eine stärkere Selbstkontrolle der Verarbeitungen durch den Betroffenen aufgefangen werden kann. Hierzu müssen den von der Datenverarbeitung Betroffenen aber Mittel an die Hand gegeben werden, damit sie diese Kontrolle effektiver als heute ausüben und ihre Rechtsdurchsetzung ökonomisch betreiben können. Das datenschutzrechtliche Instrumentarium könnte bspw. durch die Realisierung zivilrechtlicher Ansprüche der Betroffenen selbst oder entsprechender Schutzorganisationen (z.B. Bürgerrechtsvereine, Verbraucherverbände) gegenüber den verantwortlichen Betreibern von UC-Systemen unterstützt werden.[503]

Nach dem Datenschutzrecht bestehende Schadensersatzansprüche[504] werden bislang äußerst selten geltend gemacht. Hintergrund ist, dass der Bundesgesetzgeber bislang einem Vorschlag der EG-Datenschutzrichtlinie nicht gefolgt ist, eine verschuldensunabhängige Haftung des Datenverarbeiters einzuführen.[505] Eine solche Regelung wäre aber unabdingbar, weil der Betroffene im Unterschied zu dem Betreiber des UC-Systems keine Kenntnisse über die Struktur und Funktionsweise des Verarbeitungssystems hat und sich somit einem für ihn unkalkulierbaren Prozessrisiko ausgesetzt sieht. Aus demselben Grund ist auch eine Erleichterung des Nachweises der Kausalität eines Schadens zu Gunsten der Betroffenen erforderlich.[506] Ein weiterer Schwachpunkt der bisherigen Haftungsregelung ist, dass über § 7 BDSG gegenüber nicht-öffentlichen Stellen immaterielle Schäden nicht geltend gemacht werden

[503] Vgl. hierzu auch das Konzept einer „nutzerzentrierten Gefährdungshaftung“ s.u.

[504] §§ 7 f. BDSG.

[505] Siehe Art. 23 Abs. 1 EG-Datenschutzrichtlinie 95/46/EG. Zum Ganzen Simitis in: Simitis, BDSG-Kommentar, § 7, Rn. 4; Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, S. 178 ff.

[506] Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, S. 181 f.

können.[507]

Eine präventive Wirkung kann auch der Einführung eines Strafschadensersatzes für Persönlichkeitsrechtsverletzungen (punitive damages) zukommen. Das deutsche Haftungsrecht kennt derartige ausdrückliche Ansprüche, die nicht nur eine Kompensation des tatsächlich entstandenen Schadens anstreben, sondern auch Strafcharakter für den Rechtsverletzer haben sollen, bislang nicht. Solche Ansprüche sind aber in der Lage, die Verletzung der Datenschutzrechte für Unternehmen wirtschaftlich unattraktiv zu gestalten. Voraussetzung ist allerdings, dass der Betroffene über hinreichende Erfolgsaussichten und damit über einen Anreiz verfügt, die Verletzung seiner Rechte geltend zu machen. Übertreibungen, wie sie aus amerikanischen Haftungsprozessen bekannt sind, können durch eine begrenzende gesetzliche Ausgestaltung vermieden werden. Auch eine vollständige Ausschüttung der Schadensersatzsumme an den Geschädigten ist nicht zwingend. Ein Einsatz für Wiedergutmachungszwecke oder strukturelle Verbesserungen wäre ebenso denkbar.

Die Rechtsdurchsetzung der Betroffenen kann wirksam durch eine Stärkung der verbraucherrechtlichen Verbandsklage unterstützt werden. Mit diesem Instrument setzten anerkannte Verbraucherverbände die Rechte von Verbrauchern im Wege einer Klage gegenüber einzelnen Unternehmen durch. Dieses Instrument ist vor allem im Bereich der gerichtlichen AGB-Kontrolle wirksam, in deren Rahmen regelmäßig auch Datenschutzklauseln überprüft werden. Für eine weitergehende Durchsetzung von Datenschutzrechten bedarf es jedoch einer ausdrücklichen Aufnahme des Datenschutzrechts in den Katalog der im Wege der Verbandsklage zu verfolgenden Verbraucherrechte.[508]

Wie oben bereits dargelegt, sind umfassende Informations- und Auskunftspflichten zur Stärkung des Betroffenen im UC-Umfeld erforderlich. Einer umfassenden Information bedürfen die Betroffenen auch, wenn sie wirksam in die Erhebung und Verarbeitung ihrer Daten vor dem Betreten eines UC-Anwendungsraumes einwilligen sollen. Wenn – wie dargestellt – eine Einwilligung in eine einzelne konkrete Datenverarbeitung unter praktischen Gesichtspunkten ausgeschlossen ist, kann sie sich nur auf die Erhebungen und Verarbeitungen im Rahmen eines Nutzungsverhältnisses beziehen. Die Informationen müssen sich in diesen Fällen auf ein umfassendes Verständnis des Systems beziehen.[509] Der Betroffene muss über die verantwortliche(n) Stelle(n), die zu erhebenden personenbezogenen Daten, den Verwendungszweck, die Empfänger, das Hintergrundsystem der Verarbeitung einschließlich ihrer Logik und Kriterien, die Auswertung seiner Daten, die Kombination mit weiteren Daten und deren Herkunft sowie mögliche Entscheidungskriterien informiert werden, soweit das System ihn betreffende Entscheidungen fällt oder vorbereitet. Die Formulierung und Gestal-

[507] Siehe Simitis in: Simitis, BDSG-Kommentar, § 7 Rn. 32. Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, S. 182 f.

[508] Siehe § 2 UKlaG.

[509] Einen ersten Regelungsansatz bietet § 291 a Abs. 3 Satz 2 SGB V zur elektronischen Gesundheitskarte. Danach ist der Versicherte von der Krankenkasse „umfassend und in allgemein verständlicher Form über deren Funktionsweise, einschließlich der Art der auf ihr oder durch sie zu erhebenden, zu verarbeitenden oder zu nutzenden Daten zu informieren“.

tung informativer und verständlicher Einwilligungserklärungen wird die Praxis vor neue Herausforderungen der Kommunikation stellen. Eine gewisse Entlastung ist jedoch durch eine automatisierte Unterstützung der jeweiligen Prozesse sowie entsprechender Voreinstellungen auf der Seite der Nutzer in Anlehnung an den P3P-Standard des W3C-Konsortiums möglich.[510]

Mit der Durchdringung des Alltags mit UC-Anwendungen rückt die Frage in den Mittelpunkt, ob die Einwilligung in die personenbezogene Datenverarbeitung freiwillig erfolgt. Ausgangspunkt ist das so genannte Koppelungsverbot, wonach die Einwilligung in eine Verarbeitung nicht mit dem Angebot einer Ware oder Dienstleistung verknüpft werden darf.[511] Kritisch sind vor allem die Fälle, in denen der Verarbeiter über eine faktische Monopolstellung verfügt, so dass dem Betroffenen gar keine andere Wahl bleibt als entweder auf die Nutzung, die Ware oder die Dienstleistung zu verzichten oder seine Einwilligung in eine Datenverarbeitung zu erteilen. Unter diesen Umständen wird die Einwilligung jedoch nicht freiwillig erteilt. Übertragen auf UC-Anwendungen könnte die Situation eintreten, dass die Verbraucher Einkaufspassagen, Ladenpassagen oder öffentliche Verkehrsflächen nicht mehr betreten können, ohne in eine Erhebung ihrer personenbeziehbaren Objektdaten und deren Verarbeitung einzuwilligen. Unter diesen Umständen ist eine Einwilligung jedoch regelmäßig unfreiwillig und damit unwirksam. Ferner ist die Erhebung und Verarbeitung der Daten nur in den engen Grenzen einer gesetzlichen Grundlage der Vertragserfüllung zulässig.

6.3.5 Rechtliche Rahmenbedingungen für technische Lösungen

Die Herausforderungen für den Datenschutz ergeben sich aus einer neuen Qualität und Quantität von Datenverarbeitungen, die durch die UC-Systeme ermöglicht werden. Noch kann die Entwicklungsdynamik für datenschutzfreundliche Systeme nicht Schritt halten mit den Erfordernissen, die sich aus den individuellen und gesellschaftlichen Folgen neuer Technologien ergeben. Kern solcher technischer Lösungen für den Datenschutz ist ein benutzungsfreundliches und wirksames technikgestütztes Identitätsmanagement.[512] Da in einer allgegenwärtigen Datenverarbeitungswelt Einzellösungen keinen Erfolg versprechen, werden flankierende rechtliche Rahmenbedingungen erforderlich sein, um eine einheitliche datenschutzgerechte Infrastruktur zu schaffen. So werden Standards und Interoperabilitätsanforderungen definiert werden müssen, die ein Identitätsmanagement über die Grenzen von Produkt- und Herstellergrenzen hinweg ermöglichen. Gleichzeitig bedarf es Regeln, unter welchen Voraussetzungen Einwilligungen wirksam sind, die über einen Identitätsmanager erteilt werden. Mit der Verbindlichkeit der von den Betroffenen über ihren Identitätsmanager

[510] Für die elektronische Gesundheitskarte hat der Gesetzgeber in § 291 a Abs. 3 Satz 4 SGB V vorgesehen, dass die Einwilligung des Betroffenen „bei erster Verwendung der Karte vom Leistungserbringer auf der Karte zu dokumentieren ist“.

[511] Siehe zu § 3 Abs. 4 TDDSG, Bizer in: Roßnagel, Recht der Multimediadienste, TDDSG; § 3, Rn. 194 ff; Simitis in: Simitis, BDSG-Kommentar, § 4 a, Rn. 65.

[512] Siehe oben zum Begriff Kapitel 3.1.10. Zum Stand der Forschung bzgl. Identitätsmanagement siehe auch http://www.prime-project.eu/

formulierten Vorgaben wird sich nicht nur das Datenschutzniveau in UC-Anwendungen deutlich heben lassen, sondern gleichzeitig auch die Akzeptanz der Betroffenen.

Neben der benutzerzentrierten Komponente eines Identitätsmanagements kann die Automatisierung der Kontrolle datenschutzrechtlicher Vorgaben in Behörden und Unternehmen nachhaltig zu einer verbesserten Rechtsdurchsetzung beitragen.[513] Eine vereinfachte Prüfung der Datenschutz-Policies und der Implementierung des Systems könnte auf diese Weise langwierige Einzelprüfungen von Systemen verkürzen. In einem Umfeld mit einer Vielzahl von Verarbeitungen wie beim Ubiquitous Computing stellt die Automatisierung eine wichtige Möglichkeit dar, Kontrollen durch die verantwortlichen Stellen selbst oder die Aufsichtbehörden in nennenswertem Umfang und wirtschaftlich tragbar zu realisieren. Wirksame Kontrollen und Rechtsdurchsetzung wirken sich unmittelbar positiv auf den faktischen Datenschutzstandard aus. Automatisiertes Datenschutzmanagement erfordert neben einer standardisierten technischen Plattform für den Austausch von Metainformationen auch maschinenlesbare Policies, die die rechtlichen Anforderungen widerspiegeln. Die Umsetzung von Recht in solche Policies wird durch einfache und klare rechtliche Vorschriften erleichtert, die wann immer möglich auf technisch allenfalls defizitär abbildbare Abwägungsklauseln verzichten.

Identitäts- und automatisiertes Datenschutzmanagement sind zu einer technischen Unterstützung des Betroffenen weiter zu entwickeln, damit er seine individuellen Datenschutzrechte in Form einer digitalen Rechte-Management-Technik wahrnehmen kann.[514] Voraussetzung ist jedoch, dass UC-Systeme designbedingten Beschränkungen unterliegen, die eine personenbezogene Datenverarbeitung nur unter bestimmten Voraussetzungen wie einer Einwilligung des Nutzers zulassen. Solche Vorgaben über verpflichtende Eigenschaften von UC-Systemen könnten im Wege der Standardisierung oder über rechtliche Anforderungen geschaffen werden.

Eine weitere Perspektive einer datenschutzkonformen Technikgestaltung kann sich aus der Implementierung von Pseudonymitätskonzepten ergeben. Hierbei kommt es darauf an, dass durch wirksame Schutzmechanismen einer auf mehrere Rollen verteilten Datenverarbeitung die personenbeziehbaren Objektdaten nicht einer bestimmten Person zugeordnet werden können, sondern an der Grenze zur faktischen Anonymität verbleiben, um ihre weitere Verarbeitung ohne Risiko für die informationelle Selbstbestimmung zu ermöglichen. Jedoch bedarf es gesonderter Rechtsregeln, damit im Fall von Zuordnungslisten die Identifikatoren der Betroffenen vertrauenswürdigen Institutionen übergeben und dort gegen einen unbefugten Zugriff Dritter durch strikte Regeln der Zweckbindung geschützt werden. Kombiniert mit Techniken eines Identitätsmanagers sollte die Verwaltung der Pseudonyme und der Identifikatoren der Betroffenen im Sinne des Selbstdatenschutzes in der Hand des Betroffenen liegen.

[513] Zum automatisierten Datenschutzmanagement siehe http://www.datenschutzzentrum.de/adam/; Möller, Automatisiertes Management von Datenschutzrechten, DuD 2006, S. 98.

[514] Siehe auch Möller, Automatisiertes Management von Datenschutzrechten, DuD 2006, S. 98.

6.3.6 Marktorientierte Maßnahmen zur präventiven Förderung von Datenschutz und Datensicherheit

Bereits die zuvor angesprochenen Regelungsansätze zur zivilrechtlichen Durchsetzung von Ansprüchen bei Datenschutzverstößen sollen die wirtschaftliche Motivation der verantwortlichen Stellen für ein datenschutzkonformes Verhalten erhöhen. Derartige Anreize sind aber auch im Markt für UC-Systeme und für UC-Dienstleistungen zu verankern, um Datenschutzanforderungen bereits präventiv in den Forschungs- und Entwicklungsprozess von UC-Systemen zu implementieren. Datenschutz und Datensicherheit werden so zu einem Design-Ziel der UC-Produkte, unterstützen damit aber auch gleichzeitig den Vertrieb und lassen sich mithin als Wettbewerbsvorteil gegenüber den Kunden erfolgreich einsetzen.

6.3.6.1 Zertifizierung von Produkten und Implementierungen

Um einen Zustand struktureller Verantwortungslosigkeit beim Einsatz von UC-Systemen zu Lasten der Betroffenen zu vermeiden, müssen Maßnahmen des präventiven Datenschutzes ihren Ausgangspunkt bei den Herstellern und Betreibern dieser UC-Systeme nehmen, die gleichzeitig auch die wirtschaftlichen Vorteile aus ihrer Produktion bzw. ihrem Einsatz ziehen. Eine Möglichkeit bietet eine verschärfte Haftung der Produzenten für die Datenschutzkonformität der von ihnen in den Verkehr gebrachten UC-Komponenten bzw. UC-Systeme. Einen größeren Anreiz bieten auch Mechanismen, die die Investitionen in die Datenschutzkonformität von UC-Systemen werbewirksam durch ein Zertifikat belohnen. Trotz der Bundesregelung in § 9 a BDSG bietet als einziges Land bislang Schleswig-Holstein ein Datenschutz-Gütesiegel an, mit dem datenschutzkonforme Produkte, die in der Landesverwaltung eingesetzt werden können, nach einer Prüfung durch sachverständige Gutachter vom Unabhängigen Landeszentrum für Datenschutz (ULD) ausgezeichnet werden.[515] Das Datenschutz-Gütesiegel erfreut sich bei 30 Verleihungen und weiteren noch nicht abgeschlossenen Verfahren mittlerweile einer großen Wertschätzung. Im Jahr 2004 wurde es von der Europäischen Kommission mit einem Europäischen Innovationspreis ausgezeichnet.

Von noch größerer Bedeutung ist die Auditierung von UC-Systemen, mit der die datenschutzgerechte Implementierung des gesamten Systems in seiner Anwendungsumgebung geprüft, dokumentiert und schließlich zertifiziert wird. Anknüpfungspunkt für die Zertifizierung wäre die Implementierung des UC-Systems in einem von dem Betreiber zu verantwortenden Anwendungsraum („Verwantwortungsraum“) einschließlich des dazu gehörenden Hintergrundsystems. Bislang werden lediglich in Schleswig-Holstein auf landesrechtlicher Grundlage IT-Verfahren in der Landesverwaltung mit großem Erfolg auditiert. Mangels eines Ausführungsgesetzes zu § 9 a BDSG fehlt es auch hier an einer bundeseinheitlichen Regelung für den Bereich der Wirtschaft. Eine Alternative wäre die Entwicklung eines Auditierungsschemas im Wege der internationalen Standardisierung.

[515] Näher http://www.datenschutzzentrum.de/guetesiegel/

6.3.6.2 Nutzerzentrierte Gefährdungshaftung für Verletzungen des informationellen Selbstbestimmungsrechts

Die oben (Kap. 6.3.2) bereits dargestellte Figur der Verantwortungsräume könnte im Datenschutzrecht eine Ausgestaltung in Form einer nutzerorientierten Gefährdungshaftung für Verletzungen des informationellen Selbstbestimmungsrechts finden.

Ausgangspunkt des Verantwortlichkeitsproblems im UC ist die fehlende Transparenz von Verarbeitungen und Verantwortlichkeiten. Daraus ergeben sich die Probleme, eine Verarbeitung personenbeziehbarer Daten nachzuweisen, die aufwändige Kontrolle von ganzen UC-Systemen sowie Defizite in der Rechtsdurchsetzung, wenn UC-Daten grenzüberschreitend insbesondere in Drittstaaten verarbeitet werden. Diese Schwierigkeiten nehmen dem Betroffenen die Möglichkeit, sein informationelles Selbstbestimmungsrecht auszuüben und eigene Rechte effektiv durchzusetzen. Um dem informationellen Selbstbestimmungsrecht in UC-Systemen Wirkung zu verleihen, müssen Rahmenbedingungen geschaffen werden, die dem Nutzer trotz der komplexen Verarbeitungssysteme seine Entscheidungs- und Handlungsmöglichkeiten zurückgeben. Eine Grundbedingung ist die Realisierung von einfacheren Formen der Verantwortungszuweisung durch die Einführung einer Gefährdungshaftung für den Betrieb von UC-Systemen.

Anleihen können aus mit UC-Systemen vergleichbaren Sachverhalten genommen werden, bei denen sich systemimmanente Risiken für die Rechtsgüter Dritter aus der Betriebsgefahr des Systems ergeben. Diese resultiert regelmäßig aus der Komplexität der Technik, aber auch aus der Potenzierung von Risiken im Massenverkehr. Um Zustände einer strukturellen Verantwortungslosigkeit und damit Schutzlücken für die Opfer von fehlerhaften Produkten und Systemen sowie dem Betrieb von Maschinen zu vermeiden, hat der Gesetzgeber in diesen Fällen eine grundsätzliche Verantwortlichkeit derjenigen Personen festgeschrieben, ohne deren Mitwirkung sich die dem Produkt oder System inhärente Betriebsgefahr nicht realisieren könnte. Dies ist der Produzent bzw. der Importeur sowie der Halter bzw. Betreiber. Im Fall der Produzentenhaftung haftet der Produzent oder Importeur bspw. unabhängig von einen etwaigen Verschulden[516], wenn ein Fehler an dem Produkt einen Schaden verursacht.[517] Eine verschuldensunabhängige Regelung gilt auch nach dem Straßenverkehrsgesetz[518] oder nach dem Umwelthaftungsgesetz.[519] Im letzten Fall hat der Gesetzgeber dar-

über hinaus eine Kausalitätsvermutung zu Lasten des Betreibers festgelegt, wenn die Anlage nach den Gegebenheiten des Einzelfalles wie bspw. dem Betriebsablauf für die Verursachung des Schadens geeignet ist.[520] Eine vergleichbare Konstruktion gilt für Schäden, die durch gentechnisch veränderte Mikroorganismen ausgelöst werden.[521] Diese Beispiele zeigen, dass der Gesetzgeber rechtssystematisch bei technischen Sachverhalten im Massenverkehr nicht nur eine Gefährdungshaftung, sondern darüber hinaus bei verdeckten Schadensverläufen auch eine Beweiserleichterung für die Kausalität des Schadensverlaufes vorgesehen hat. Eine vergleichbare Regelung fehlt bislang lediglich für den Bereich des immateriellen Datenschutzrechts. Angesichts der Komplexität der Verarbeitungsabläufe sowie der

[516] Vorsatz oder Fahrlässigkeit, d.h. Verletzung von Sorgfaltspflichten.

[517] Siehe § 1 Abs. 1 ProdHaftG: „Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen."
Abs. 4: „Für den Fehler, den Schaden und den ursächlichen Zusammenhang zwischen Fehler und Schaden trägt der Geschädigte die Beweislast. Ist streitig, ob die Ersatzpflicht gemäß Absatz 2 oder 3 ausgeschlossen ist, so trägt der Hersteller die Beweislast."

[518] § 7 Abs. 1 StVG: „Wird bei dem Betrieb eines Kraftfahrzeugs oder eines Anhängers, der dazu bestimmt ist, von einem Kraftfahrzeug mitgeführt zu werden, ein Mensch getötet, der Körper oder die Gesundheit eines Menschen verletzt oder eine Sache beschädigt, so ist der Halter verpflichtet, dem Verletzten den daraus entstehenden Schaden zu ersetzen."

[519] § 1 UHaftG: „Wird durch eine Umwelteinwirkung, die von einer im Anhang 1 genannten Anlage ausgeht, jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Inhaber der Anlage verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen."

[520] § 6 Abs. 1 UHaftG: „Ist eine Anlage nach den Gegebenheiten des Einzelfalles geeignet, den entstandenen Schaden zu verursachen, so wird vermutet, dass der Schaden durch diese Anlage verursacht ist. Die Eignung im Einzelfall beurteilt sich nach dem Betriebsablauf, den verwendeten Einrichtungen, der Art und Konzentration der eingesetzten und freigesetzten Stoffe, den meteorologischen Gegebenheiten, nach Zeit und Ort des Schadenseintritts und nach dem Schadensbild sowie allen sonstigen Gegebenheiten, die im Einzelfall für oder gegen die Schadensverursachung sprechen."

[521] §§ 32 Abs. 1, 34 GenTG.

verdeckten Verarbeitungen ist eine solche Regelung jedoch überfällig.[522] Derartige Haftungsregelungen sind auch ökonomisch sinnvoll, weil sie die Verantwortung nicht nur beim Verursacher eines konkreten Schadens, sondern auch bei demjenigen verorten, der die wirtschaftlichen Vorteile für das Inverkehrbringen des Produktes oder Verfahrens zieht sowie Einfluss auf eine Gefahren vermeidende Gestaltung nehmen kann.

Im Fall eines UC-Systems muss die Zurechnung der Verantwortung an der Betriebsgefahr ansetzen, die durch den Betrieb des UC-Systems für die informationelle Selbstbestimmung der Betroffenen ausgelöst wird. Durch die Einrichtung einer Gefährdungshaftung müsste der Betroffene dem Betreiber weder Vorsatz noch Fahrlässigkeit nachweisen. Eine gesetzliche Ursachenvermutung sollte den Betroffenen im Fall eines UC-Systems auch von dem Nachweis der Kausalität zwischen der konkreten Verarbeitung und seinem Schaden entlasten. In diesem Fall hätte der Betreiber des UC-Systems nachzuweisen, dass sein System datenschutzkonform personenbeziehbare Objektdaten erhebt bzw. eine Zuordnung zu den Betroffenen vornimmt. Den Nachweis einer derartigen Datenschutzkonformität könnte der Betreiber über eine Datenschutzkontrolle im Einzelfall, insbesondere aber durch eine Vorabkontrolle des UC-Systems sowie einer Auditierung der laufenden Implementierung, erbringen. Eine Enthaftung des Betreibers setzt einen Nachweis voraus, dass die notwendige Basisprävention gegen mögliche Rechtsverletzungen ergriffen worden ist.

Voraussetzung für die Wirksamkeit dieser Verantwortungszuweisungen ist jedoch, dass immaterielle Schäden im Unterschied zu heute im Wege des Schadensersatzes auch gegenüber nicht-öffentlichen Stellen liquidiert werden können.

Soweit der Betreiber für den Schaden nicht selbst verantwortlich ist, kann er im Innenverhältnis seinen Schaden gegenüber den ihm bekannten Teilverantwortlichen geltend machen. Den Betroffenen würde eine solche Regelung von dem Nachweis der in dem UC-System erfolgenden Verarbeitungsvorgänge entlasten. Eine solche Verlagerung der Verantwortung ist interessengerecht, da der Betreiber des UC-Systems die an dem System Beteiligten im Unterschied zu dem Betroffenen regelmäßig kennen wird. Letztlich geben die genannten Grundzüge eines Systems der Verantwortungszuweisung eine Form erweiterter Verkehrssicherungspflichten des Betreibers von UC-Systemen wieder.

Für die Wirksamkeit der Verantwortungsregelungen sind ihre marktbedingten Nebeneffekte von Bedeutung. Eine verschuldensunabhängige Haftung führt in der Regel dazu, dass die Betreiber ihre Risiken versichern, wobei die Versicherung die Höhe der Prämien an der von dem Betreiber getroffenen Risikovorsorge orientiert. Hierzu gehört neben einer ordnungsgemäßen Konzeptionierung der Datenverarbeitung in der UC-Anwendung auch die Entlastung über den Erwerb datenschutzkonformer Produkte sowie den Nachweis eines ordnungsgemäßen Betriebes. So werden die Betreiber, um ihre Haftungsrisiken zu minimieren, bei ihren Lieferanten datenschutzkonforme Produkte bzw. datenschutzkonforme Standardkonfigurationen einfordern. Diese können durch Produkt-Zertifikate wie das Datenschutz-

[522] Simitis in: Simitis, BDSG-Kommentar, § 7, Rn. 4 ff.; Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, S. 178 ff.

Gütesiegel kommuniziert und als Wettbewerbsvorteil des Produzenten bzw. Lieferanten eingesetzt werden und auf diese Weise die Verbreitung von Privacy Enhancing Technologies (PET) fördern. Die UC-Betreiber werden vor allem eine Auditierung ihrer UC-Systeme in der konkreten Anwendung anstreben, um im Falle einer Rechtsverletzung einerseits einen Nachweis der Enthaftung führen und andererseits dem Kunden ein Merkmal der eigenen Seriosität als vertrauensbildende Maßnahme anbieten zu können.

6.4 Zusammenfassung

Viele der durch UC-Systeme aufgeworfenen Rechtsprobleme sind nicht grundlegend neu, sie werden durch die Verbreitung von UC-Systemen aber noch zusätzlich verschärft. Ihre Wurzeln liegen in der fortschreitenden Miniaturisierung und Vernetzung der Verarbeitung personenbezogener Daten begründet, die mit der Entwicklung von verteilten und vernetzten UC-Anwendungen eine weitere Stufe erreicht. Die Probleme eines wirksamen Datenschutzes für UC-Anwendungen werden durch die Verlagerung von Verarbeitungsschritten in andere Länder, insbesondere unsichere Drittstaaten, noch weiter vertieft. Folgende wesentliche Risiken und Möglichkeiten des Risikomanagements ergeben sich im Einzelnen.

6.4.1 Rechtsdurchsetzung

Für den Betroffenen ist die Geltendmachung seiner Rechte nur attraktiv, wenn diese mit angemessenem Aufwand möglich und kurzfristig verfügbar ist und kein übermäßiges Kostenrisiko bedeutet. Insbesondere der Zeitfaktor wird angesichts der Vielzahl permanent stattfindender Verarbeitungen und der zu erwartenden Innovationsgeschwindigkeit von UC-Systemen für einen effektiven Rechtsschutz bedeutend sein.

Die Durchsetzung der Datenschutzrechte zu Gunsten der Betroffenen kann erheblich verbessert werden, wenn das Eigeninteresse der Betreiber von UC-Systemen gestärkt wird. Dies lässt sich z.B. durch die Einführung einer nutzerzentrierten Gefährdungshaftung der Betreiber von UC-Systemen erreichen. Voraussetzung ist jedoch die Einführung eines Anspruches auf Ersatz eines immateriellen Schadens für die Verletzung des informationellen Selbstbestimmungsrechts bzw. des Persönlichkeitsrechts des Betroffenen.

6.4.2 Datensparsame Technikgestaltung

Vorbeugende Schutzmaßnahmen werden eine wesentliche Rolle für den Datenschutz in UC-Systemen spielen müssen. Dazu gehört eine datensparsame zweckorientierte Technikgestaltung ebenso wie datenschutzfreundliche Voreinstellungen von Anwendungen in UC-Systemen. Sie ergeben sich aus der Verpflichtung zur Wahrung der gesetzlich geregelten Datenschutzrechte und können durch ökonomische Erwägungen der Betreiber von UC-Systemen unterstützt werden. Die UC-Betreiber können zum einen durch die Nachfrage der Kunden und Verbraucher nach datenschutzfreundlichen UC-Anwendungen angeregt werden. Für sie kann aber auch von Bedeutung sein, dass sich das Risiko von Persönlichkeits-

verletzungen aus dem Betrieb ihres UC-Systems in Haftungsrisiken niederschlägt, denen es durch eine datenschutzkonforme Technikgestaltung und –anwendung vorzubeugen gilt. Müssen diese durch Versicherungen abgedeckt werden, entsteht eine zusätzliche Motivation, die zum Betrieb datenschutzfreundlicher UC-Produkte und Dienstleistungen beiträgt.

6.4.3 Zweckbindung

Der datenschutzrechtliche Grundsatz der Zweckbindung ist für die Verarbeitung personenbezogener Daten in UC-Systemen von erheblicher Bedeutung, da sie eine umfassende Profilbildung über das Verhalten des Betroffenen ermöglichen. Solche Profile haben im Regelfall einen großen wirtschaftlichen Wert, so dass ein entsprechendes Verwertungsinteresse grundsätzlich in die Risikobetrachtung einbezogen werden muss. Die Generierung und Verwendung von Nutzungs- und Verhaltensprofilen aus UC-Systemen ist ohne eine ausdrückliche Zustimmung des Betroffenen rechtswidrig. Angesichts der gegenläufigen wirtschaftlichen Interessen sollte eine rechtswidrige Verarbeitung und Nutzung der im Rahmen von in UC-Systemen entstandenen Profildaten deutlich sanktioniert werden. Dies wäre de lege lata über Regelungen zum Strafschadensersatz möglich, aber auch durch eine normenklare Sanktionierung entsprechender Normverstöße in die datenschutzrechtlichen Bußgeldtatbestände bzw. bei einer entsprechenden Bereicherungsabsicht auch in die Strafvorschriften. Die Rechtsdurchsetzung liegt im Übrigen in den Händen der Aufsichtsbehörden, deren wirksame Tätigkeit eine entsprechende personelle Ausstattung voraussetzt.

6.4.4 Transparenz

Datenschutzrechtlich ist den Betroffenen eine umfassende Transparenz der Verarbeitungsvorgänge ihrer Daten in UC-Systemen zu gewährleisten. Insbesondere weil eine Vielzahl unsichtbarer und parallel stattfindender Verarbeitungen eine detaillierte Information im Einzelfall kaum zulassen wird (Ökonomie der Aufmerksamkeit), gewinnt eine verständliche und nachvollziehbare Aufklärung bspw. über die systematischen Zusammenhänge der Verarbeitungen und der verwendeten Daten und Kriterien innerhalb bestimmter räumlicher Bereiche und begrenzter Zeithorizonte an Bedeutung. Derartige systematische Unterrichtungen werden in UC-Systemen die Wissensbasis für selbstbestimmte Entscheidungen des Betroffenen bilden müssen.

Der Betroffene muss aber nicht nur unterrichtet werden, sondern er muss auch seinen Auskunftsanspruch wirksam wahrnehmen können. Hierzu ist ihm in Anlehnung an die Services bestehender Onlinedienste die Möglichkeit zu geben, vor Ort, über das Internet oder andere ihm ohne weiteren Aufwand erreichbare Mittel, ein „Datenkonto“ mit den über ihn im Rahmen des UC-Systems zu seiner Person verarbeiteten Daten bereit zu stellen. Er sollte darüber hinaus über die Möglichkeit verfügen, personenbeziehbare Objektdaten aus der Nutzung des UC-Systems zu löschen. Die Betreiber eines UC-Systems haben die Betroffenen auf den Betrieb von Lesegeräten bzw. Sensoren hinzuweisen und eine Stelle anzugeben, an die sie sich zur Wahrnehmung ihrer Datenschutzrechte wenden können.

6.4.5 Verantwortlichkeiten

Der räumliche und zeitliche Einsatz von UC-Anwendungen erfordert finanzielle Aufwendungen, über die in Organisationen die verantwortlichen Entscheidungsträger zu befinden haben. Entsprechendes gilt auch für die konkrete Installation und den Betrieb von UC-Anwendungen, so dass die Verarbeitung für den Betroffenen zwar heimlich und intransparent erfolgt, aber von den entsprechenden Stellen zu verantworten ist. Verantwortlich für die Rechtmäßigkeit der Erhebung von personenbeziehbaren Objektdaten ist im Regelfall der Betreiber des Hintergrundsystems, in dem die Lesegeräte und Sensoren miteinander verknüpft sind. Dieser wird im Regelfall personenbezogene Daten in definierten „Räumen“ für eigene Zwecke erheben und verarbeiten und trägt insoweit auch die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung. Neben dem für das Hintergrundsystem Verantwortlichen kommt auch der Inhaber des Hausrechts als Verantwortlicher in Betracht, wenn er eine heimliche oder offene Erhebung personenbeziehbare Objektdaten veranlasst oder in seinen Räumlichkeiten duldet. Werden personenbezogene Daten auf den Mikrochips der Objekte gespeichert, dann sind in Anlehnung an § 6 c Abs. 1 BDSG die Stellen für die Datenverarbeitung verantwortlich, die den Datenträger ausgegeben bzw. ihn programmiert haben.

6.4.6 Internationalität und Outsourcing

Erfolgt die Datenverarbeitung in UC-Systemen durch Betreiber mit Sitz in mehreren Ländern, so ist sie für das Gesamtsystem mangels eines international einheitlichen Datenschutzstandards auf das nach der EG-Datenschutzrichtlinie zulässige Schutzniveau zu begrenzen. Die Kontrolle und Durchsetzung dieser Anforderung wird angesichts des Umfangs der Verarbeitungen und der nur begrenzten Möglichkeiten einer einfachen Rechtsdurchsetzung im Ausland problematisch bleiben.

6.4.7 Rechtliche Rahmenbedingungen technischer Schutzmechanismen

Eine zentrale Rolle zur Vermeidung von Datenschutzrisiken wird der Entwicklung und Implementierung von Mechanismen des Identitätsmanagements zu kommen, das die Betroffenen u.a. bei der Abgabe und Verwaltung von Einwilligungserklärungen unterstützt. Kombiniert mit Pseudonymitätskonzepten sollte es Ziel einer solchen Gestaltung sein, die Verarbeitung von personenbezogenen Objektdaten durch zusätzliche Schutzmechanismen zu ermöglichen, ohne die informationelle Selbstbestimmung der Betroffenen zu gefährden.

Zur Förderung und Implementierung derartiger Mechanismen bedarf es flankierender normativer Rahmenbedingungen. Hierzu gehören neben Anforderungen der Standardisierung und der Interoperabilität, die ein Identitätsmanagement über Produkt- und Herstellergrenzen hinweg ermöglichen, auch Regelungen, die den maschinell unterstützten Einwilligungserklärungen nicht nur eine bindende Wirkung zukommen lassen, sondern auch ihre Einhaltung kontrollieren können. Eine solche Rechtssicherheit bspw. für die Wirksamkeit von Einwilligungserklärungen, die mit Unterstützung eines Identitätsmanagers erteilt werden, wird sich auch positiv auf die Akzeptanz solcher Systeme bei den Nutzern von UC-Systemen auswirken.

Eine Automatisierung der Kontrolle datenschutzrechtlicher Vorgaben wird nachhaltig zu einer verbesserten Durchsetzung der Datenschutzrechte beitragen. In einem Umfeld mit einer Vielzahl von Verarbeitungen in UC-Systemen stellt die Automatisierung eine wichtige Möglichkeit dar, Kontrollen durch die verantwortlichen Stellen selbst, die Betroffenen oder die Aufsichtbehörden in nennenswertem Umfang und wirtschaftlich tragbar zu realisieren. Wirksame Kontrollen und Rechtsdurchsetzung fördern einen faktischen Datenschutzstandard unmittelbar. Automatisiertes Datenschutzmanagement erfordert neben einer standardisierten technischen Plattform für den Austausch von Metainformationen auch maschinenlesbare Policies, die die rechtlichen Anforderungen erfüllen.

6.5 Literatur

Art. 29 Gruppe: Arbeitsdokument zu 'Datenschutz und RFID-Technologien', http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_de.pdf

Art. 29 Gruppe: Ergebnisse der öffentlichen Anhörung zum Arbeitspapier 105 der Art. 29 Arbeitsgruppe zum Thema Datenschutz und RFID-Technologie, http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_de.pdf

Barthel, Thomas: RFID-Anwendungen im Betrieb und bei Arbeitnehmerdaten, Datenschutznachrichten (DANA) 03/2004, S. 5-9.

Borchert, Günter: Verbraucherschutzrecht, München 1994.

Büllesbach, Alfred / Löss, Petra: Vertragslösung, Safe Harbor oder Privacy Code of Conduct, Datenschutz und Datensicherheit (DuD) 2002, S. 135-138.

Bundesregierung: Keine Gefahr für Datenschutz beim Einsatz von Radiofrequenztechnik, MultiMedia und Recht (MMR) 07/2004, S. X.

Bundesverfassungsgericht (BVerfG): „Volkszählung“, BVerfGE 65, S. 1 ff.

Bundesverfassungsgericht (BVerfG): Verwertung von Erkenntnissen aus einer GPS-Observation, MultiMedia und Recht (MMR) 2005, S. 371.

Conrad, Isabell: RFID-Ticketing aus datenschutzrechtlicher Sicht, Computer und Recht (CR) 2005, S. 537 ff.

Däubler, Wolfgang: Computersysteme im Handel – rechtliche Rahmenbedingungen für den Betriebsrat, in: Die Zukunft im Handel hat begonnen! RFID, PEP, Loss Prevention & Co, Dokumentation zur Fachtagung der BTQ Kassel und ver.di Fachbereich Handel, 15.-17. November 2004, S. 33-38.

Deutsch, Erwin: Die neuere Entwicklung der Rechtsprechung zum Haftungsrecht, Juristenzeitung (JZ) 2005, S. 987-994.

Deutscher Bundestag: Eintrittskarten zur Fußball-Weltmeisterschaft 2006 und Datenschutz (kleine Anfrage), Bundestagsdrucksache 15/4896 vom 16.02.2005.

Deutscher Bundestag: Eintrittskarten zur Fußball-Weltmeisterschaft 2006 und Datenschutz (Antwort der Bundesregierung), Bundestagsdrucksache 15/5011 vom 07.03.2005.

Eisenberg, Ulrich / Puschke, Jens / Singelnstein, Tobias: Überwachung mittels RFID-Technologie, ZRP 01/2005, S. 9-12.

Gnirck, Karen / Lichtenberg, Jan: Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen, DuD 2006, S. 598-602.

Gola, Peter / Wronka, Georg: Handbuch zum Arbeitnehmerdatenschutz, 3. Aufl., Frechen 2004.

Gola, Peter / Schomerus, Rudolf: BDSG, Bundesdatenschutzgesetz, Kommentar, 8. Aufl., München 2004.

Hansen, Marit / Wiese, Markus: Gateway, RFID – Radio Frequency Identification, Datenschutz und Datensicherheit (DuD) 2004, S. 109.

Heise Newsticker: Pervasive 2005: Realitätsabgleich, http://www.heise.de/newsticker/meldung/59440 (10.05.2005).

Heise Newsticker: Bundesdatenschützer will keine gläsernen Autofahrer, http://www.heise.de/newsticker/meldung/71439 (29.03.2006).

Heise Newsticker: IBM schlägt datenschutzgerechte RFID-Chips vor, http://www.heise.de/newsticker/meldung/70778 (13.03.2006).

Heise Newsticker: Forscher präsentieren Vorläufer des elektronischen Staubs, http://www.heise.de/newsticker/meldung/63145 (23.08.2005).

Hoenike, Mark / Hülsdunk, Lutz: Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwil-

ligung?, MultiMedia und Recht (MMR) 2004, S. 788 ff.

Hoeren, Thomas: Privacy, Direktmarketing und das neue UWG, Datenschutz und Datensicherheit (DuD) 2004, S. 611-616.

Hoeren, Thomas: Skript zum Informationsrecht, Stand März 2005, http://www.uni-muenster.de/Jura.itm

Holznagel, Bernd / Bonnekoh, Mareike: Radio Frequency Identification – Innovation vs. Datenschutz?. MultiMedia und Recht (MMR) 2006, S. 17-23.

Hülsmann, Werner: RFIDs – Bleibt der Datenschutz auf der Strecke?, Datenschutznachrichten (DANA) 04/2004, S. 11-15.

Internationale Konferenz der Datenschutzbeauftragten: Entschließung zu Radio-Frequency Identification vom 20.11.2003, http://www.privacyconference2003.org/resolutions/RFIDResolutionGE.doc

ISTAG (Ducatel, K, Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J-C.): Scenarios for Ambient Intelligence in 2010 – Final Report, February 2001, http://www.cordis.lu/ist/istag.htm

Jacob, Joachim / Jost, Tanja, Marketingnutzung von Kundendaten und Datenschutz – ein

Widerspruch? Datenschutz und Datensicherheit (DuD) 2003, S. 621 ff.

Kelter, Harald, Widmann, Stefan: Radio Frequency Identification - RFID , Datenschutz und Datensicherheit (DuD) 2004, S. 331-334.

Koenig, Christian / Loetz, Sascha / Neumann, Andreas: Telekommunikationsrecht, Heidelberg 2004.

Köbele, Bernd: Anspruch auf Mitteilung des Anschlussinhabers bei bekannter IP-Adresse, DuD 2006, S. 609-610.

Lahner, Claus Mauricio: Anwendung des § 6 c BDSG auf RFID, Datenschutz und Datensicherheit (DuD) 2004, S. 723-726.

Landesarbeitskreis Demokratie & Recht von Bündnis90/Die Grünen Bayern: Gebrauch von RFID-Chips reglementieren, Resolution vom 23.03.2005, http://www.bayern.gruene-partei.de/cms/themen/dokbin/67/67416.rfid_chips_reglementieren_maerz_2005.pdf

Langheinrich, Marc: Die Privatsphäre im Ubiquitous Computing, http://www.vs.inf.eth.ch/publ/papers/langhein2004rfid.pdf

Medicus, Dieter: Bürgerliches Recht, 20. Aufl., Köln 2004.

Meyer, Jan-Bernd: Wie RFID funktioniert – und wie nicht, Computerwoche 25/2005, S. 22-23.

Möller, Jan: Automatisiertes Management von Datenschutzrechten, Datenschutz und Datensicherheit (DuD) 2006, S. 98-101.

Möller, Jan / Florax, Björn-Christoph: Datenschutzrechtliche Unbedenklichkeit des Scoring von Kreditrisiken? NJW 2003, S. 2724-2726.

Möller, Jan / Florax, Björn-Christoph: Kreditwirtschaftliche Scoring-Verfahren, MultiMedia und Recht (MMR) 2002, S. 806-810.

Müller, Jürgen: Ist das Auslesen von RFID-Tags zulässig? – Schutz von RFID-Transponderinformationen durch § 86 TKG, Datenschutz und Datensicherheit (DuD) 2004, S. 215-217.

Müller, Jürgen, Handy, Matthias: RFID und Datenschutzrecht, Risiken, Schutzbedarf und Gestaltungsideen, Datenschutz und Datensicherheit (DuD) 2004, S. 655-659.

Ohlenburg, Anna: Der neue Telekommunikationsdatenschutz, MultiMedia und Recht (MMR) 2004 S. 431 ff.

Otten, Geelke, Zweckbindung im Autobahnmautgesetz, DuD 2006, S. 657-660.

Palandt, Bürgerliches Gesetzbuch, 61. Aufl., München 2002.

Petri, Thomas B. / Kieper, Marcus: Datenbevorratungs- und Analysesysteme in der Privatwirtschaft, Datenschutz und Datensicherheit (DuD) 2003, S. 609-613.

Petri, Thomas B.: Datenschutz in der Privatwirtschaft, in Freundesgabe für H. Bäumler, hrsg. von J.

Bizer / A. v. Mutius / T.B. Petri / T. Weichert, Innovativer Datenschutz 1992 – 2004, Kiel 2004, S. 221-238.

Räther, Philipp C.: Datenschutz und Outsourcing, Datenschutz und Datensicherheit (DuD) 08/2005, S. 461-466.

Roßnagel, Alexander, Pfitzmann, Andreas, Garstka, Hansjürgen: Modernisierung des Datemschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.

Roßnagel, Alexander, Müller, Jürgen: Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR 2004, S. 625-632

Roßnagel, Alexander: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MultiMedia und Recht (MMR) 02/2005, S. 71-75.

Saeltzer, Gerhard: Sind diese Daten personenbezogen oder nicht?, Datenschutz und Datensicherheit (DuD) 2004, S. 218-227.

Safeguards in a World of Ambient Intelligence (SWAMI) (Friedewald, Michael / Vildjiounaite, Elena / Wright, David (Hrsg.)): The brave new world of ambient intelligence: A state-of-the-art review, 2006, http://swami.jrc.es/pages/documents/SWAMI_D1_Final.pdf

Safeguards in a World of Ambient Intelligence (SWAMI) (Punie, Yves / Delaitre, Sabine / Maghiros, Ioannis / Wright, David (Hrsg.)): Dark Scenarios in ambient intelligence: Highlighting risks and vulnerabilities, 2006, http://swami.jrc.es/pages/documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf

Schaar, Peter: Datenschutz im Internet – Die Grundlagen, München 2002.

Schaar, Peter: Datenschutzbeauftragter Peter Schaar warnt vor blauäugiger RFID-Nutzung, Interview in Computerwoche 25/2005, S. 25.

Schaub, Günter: Arbeitsrechtshandbuch, 9. Aufl., München 2000.

Schoen, Thomas: Rechtliche Rahmenbedingungen zur Analyse von Log-Files, Datenschutz und Datensicherheit (DuD) 2005, S. 84-88.

Scholz, Philipp, Datenschutz bei Data Warehousing und Data Mining in: Roßnagel, Handbuch des Datenschutzrechts, München 2003, Kap. 9.2.

Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., München 2003.

Spindler, Gerald / Schmitz, Peter / Geis. Ivo: TDG – Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz, Kommentar, München 2004.

Tangens, Rena / Rosengart, Frank: BigBrotherAward 2003 – Verbraucherschutz, Datenschutznachrichten (DANA) 04/2003, S. 8-10.

Gräfin von Westerholt, Margot / Döring, Wolfgang: Datenschutzrechtliche Aspekte der Radio Frequency Identification, Computer und Recht (CR) 2004, S. 710.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, Studie im Auftrag des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz, Kiel 2005.

Wagner, Guido: Outsourcing – mit Sicherheit, Datenschutz und Datensicherheit (DuD) 03/2005, S. 130-134.

Wedde, Peter: Schutz vor versteckten Kontrollen im Arbeitsverhältnis – Die höchstrichterliche Rechtsprechung, Datenschutz und Datensicherheit (DuD) 2004, S. 21-25.

Weichert, Thilo: Datenschutzrechtliche Anforderungen an Verbraucher-Kredit-Scoring, DuD 2006, S. 582-587.

Weichert, Thilo: Identitätskarten – sind Sicherheit und Datenschutz möglich?, http://www.datenschutzzentrum.de/vortraege/050428_weichert_alcatel.htm vom 29.04.2005.

Weichert, Thilo: Die Fußball-WM als Überwachungs-Großprojekt, Datenschutznachrichten (DANA) 01/2005, S. 7-11.

Weis, Stephen August: Security and Privacy in Radio Frequency Identification Devices, 2003, http://http://theory.lcs.mit.edu/~cis/theses/weis-masters.pdf

Weiser, Mark: The Computer for the 21st Century, http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html (11.05.2005).

Zilkens, Martin: Datenschutz am Arbeitsplatz, Datenschutz und Datensicherheit (DuD) 2005, S. 253-261.

7 Technische und organisatorische Lösungen

Benjamin Fabian, Markus Hansen[523]

7.1 Technikgestaltung des Ubiquitous Computing

Wie sollte Ubiquitous Computing gestaltet sein, um dem Individuum nicht nur erweiterte Möglichkeiten der Selbstentfaltung und bequeme Steuerung seiner Umwelt zu bieten, sondern auch umgekehrt die erhöhte Steuerbarkeit des Individuums durch diese Umwelt zu vermeiden?

Durch die Verschmelzung von Informationstechnik und physischer Umwelt wird eine stetig zunehmende Kongruenz von physischer und informationeller Selbstbestimmung des Menschen im Ubiquitous Computing (UC) bewirkt.

Die zentralen Anforderungen an UC, die sich als abstrakte, aber durch ihre Schlichtheit um so eingängigere Gegenentwürfe zu den Schattenseiten der vorgestellten Szenarien kristallisieren, sind Sicherheit und Offenheit der Technik sowie die Selbstbestimmung des sich ihr bewusst anvertrauenden oder möglicherweise unvermeidbar ausgesetzten Individuums.

In den folgenden Abschnitten identifizieren wir zentrale technische und organisatorische Lösungsansätze und diskutieren, inwieweit sie zur Umsetzungen dieser Anforderungen in der Praxis geeignet sind. Wegen ihrer Vorreiterrolle im UC und ihres zumindest partiell paradigmatischen Charakters wird die RFID-Technologie im Folgenden einen großen Raum einnehmen, wobei hier und an anderem Ort[524] auch auf andere Technologien eingegangen wird.

7.2 Technische Sicherheit im Ubiquitous Computing

7.2.1 Physische Sicherheit

Die physische Sicherheit eines Menschen, der eine UC-Umgebung nutzt, wird ohne Zweifel ein automatisches Gestaltungsziel für jedes UC-System sein, das Verbindung zu Menschen hat. Doch gerade das Grundparadigma des UC, Systeme möglichst adaptiv, besonders auch eigenständig lernend und autonom entscheidend zu gestalten, könnte bisher ungeahnte Probleme mit sich bringen, den jeweils aktuellen Systemzustand festzustellen und zu prüfen, ob er sich innerhalb der ursprünglichen Spezifikationen befindet. Bei hoher Komplexität, offener Vernetzung und ständigem Reagieren auf Nutzereingaben und andere Parameter der realen Welt wird die Vorhersage von Systemzuständen äußerst kompliziert. D.h., bereits in einem idealen regulären Betrieb ohne aktive Angreifer wird die Garantie der physischen Si-

[523] Themen Reisepass (Kap. 7.2.3.2.5.1) und Identitätsmanagement (Kap. 7.3.5).

[524] Vgl. Kapitel 1.

cherheit der Nutzer in allen Systemzuständen sehr schwierig. Aus diesem Grund muss im UC das Vorsorgeprinzip[525] verstärkt berücksichtigt werden.

Mit dem Eindringen der virtuellen Welt in die physische – visionär beschrieben mit den Bildern von „Verkörperter Virtualität“ (Embodied Virtuality[526]) und einem sogenannten Internet der Dinge – kommt als zusätzliche Erschwernis hinzu, dass sich mangelnde Informationssicherheit direkt auf die physische Sicherheit der Nutzer von UC-Systemen auswirken kann. So können solche Systeme beispielsweise aufgrund von Angriffen aus der „virtuellen Welt“ chaotisch oder unter fremder Kontrolle agieren, vielleicht sogar überlastet werden und ihren Dienst völlig einstellen.

Da man davon ausgehen kann, dass Hersteller und Betreiber von einzelnen UC-Systemen die physische Sicherheit der Nutzer in einem regulären Betrieb schon aus Haftungs- und Akzeptanzgründen sehr gründlich prüfen werden,[527] konzentrieren wir uns im Folgenden auf die Informationssicherheit von UC-Systemen, die ein wesentlicher Bestimmungsfaktor[528] ist, um überhaupt einen regulären Betrieb – und damit auch dauerhafte Akzeptanz und Wirtschaftlichkeit von Geschäftsmodellen – gewährleisten zu können.

7.2.2 Informationssicherheit

Informationssicherheit ist eine wesentliche Grundlage für die informationelle Selbstbestimmung eines Individuums in IT-Systemen[529]. Sie ist eine notwendige, aber keine hinreichende Bedingung für die Selbstbestimmung, ihre Wirkung ist ambivalent.

Notwendigkeit: Wenn ein IT-System Informationsübertragungen oder Dienste für ein Individuum so bereitstellt, dass diese von Dritten mitgehört oder manipuliert werden können, dann liegt keine objektive Selbstbestimmung des Individuums in diesem System vor, weder im informationellen noch im allgemeinen (z.B. auch physischen) Sinne.

Gegensatz: Theoretisch vor Dritten vollkommen sichere IT-Systeme können als reguläre Haupt- oder Nebenfunktion die Überwachung von Individuen beinhalten.[530] Ebenso kann durch die Berücksichtigung der Sicherheitsinteressen aller Beteiligten (multilaterale Sicherheit) ein Gegensatz zur informationellen Selbstbestimmung einzelner Systemteilnehmer ent-

[525] Hilty et al., The Precautionary Principle in the Information Society, 2005.

[526] Weiser, 1991, S. 1.

[527] Unter dem großen Caveat, dass mit zunehmender Komplexität und Wechselwirkungen von UC-Systemen untereinander Verantwortlichkeiten immer schwerer festzustellen sind, vgl. Hilty et al., 2005.

[528] Vergl. Kap. 3.

[529] Im Folgenden können auch Organisationen und juristische Personen als informationstheoretische Individuen aufgefasst werden.

[530] Zur Unterscheidung von regulären und irregulärem Systembetrieb vgl. auch AP5.

stehen, zum Beispiel durch ihre eindeutige Identifizierbarkeit.[531]

Im UC wird die Bedeutung von IT-Sicherheit gegenüber dem heutigen Internet allein schon dadurch enorm gesteigert, dass immer mehr physische Prozesse durch „virtuelle" Kommandos gesteuert werden, und IT, wie bereits dargelegt, immer mehr Einfluss auf die physische Unversehrtheit des Menschen haben wird.

Auch wird es immer schwieriger werden, sich als Individuum Computersystemen zu entziehen, wenn diese durch Angreifer kompromittiert sind – die Frage nach Machbarkeit und Design eines „Ausschaltknopfes" für UC-Systeme könnte zu einem wichtigen Teilgebiet der HCI-Forschung werden.

Bevor näher auf die speziellen Ziele von Informationssicherheit und ihre Umsetzung in die Praxis eingegangen wird, folgt zunächst im Anschluss ein Überblick über offene Systeme sowie Interaktion und Kommunikation im UC, um die Rahmenbedingungen von Informationssicherheit im UC darzustellen.

Danach diskutieren wir Probleme und Lösungsansätze in lokalen UC-Systemen (Kap. 7.2.3 mit dem Schwerpunkt RFID) und gekoppelten Internetsystemen (Kap. 7.2.4).

7.2.2.1 Offene Systeme

Zentral für die Informationssicherheit ist eine Unterscheidung von offenen und geschlossenen IT-Systemen. Die einfache und zunächst naheliegende Möglichkeit der Definition, ein geschlossenes System sei vollkommen autark und abgeschottet von anderen Systemen, ist im UC, das durch intensive Vernetzung geprägt ist, nicht realistisch und wenig fruchtbar.

Darum verstehen wir die Unterscheidung von Offenheit und Geschlossenheit im Folgenden graduell. Merkmale von geschlossenen Systemen[532] sind Homogenität, Lokalität, bekannte Betreiber und Teilnehmer, zentrale Verwaltung und im Idealfall keine oder nur sehr geringe Interaktion und Vernetzung mit anderen Systemen. Offene Systeme sind durch die jeweiligen Gegenteile charakterisiert.

Als Beispiel diene der Einsatz von RFID-Systemen in einer Bibliothek. Eine kleine Präsenzbibliothek, die zur Inventarisierung ihrer Bücher RFID-Tags mit eigenen, nur lokal benutzten Nummerncodes einsetzt und die zugehörigen Informationen in einer lokalen Datenbank hält, ist ein geschlossenes System.

Ein Verbund von Bibliotheken und Buchläden, die ein gemeinsames Nummernsystem auf RFID-Tags neben der Inventarisierung auch zu Buch- oder URL-Empfehlungen, Personalisierung und Marketingzwecken an verschiedenen Standorten nutzen, wäre ein offenes Sys-

[531] So könnte eine (theoretische) globale PKI, die überall den Internetzugang auf mehreren Netzwerkschichten regelte, möglicherweise die allgemeine Sicherheitslage im Internet erhöhen, die Privatsphäre des Individuums allerdings durch die Protokollierbarkeit, Identifizierbarkeit und Nichtbestreitbarkeit jeder Interaktion zunichte machen. Zu diesem Gegensatz und Lösungsansätzen siehe z.B. Chaum, 1985; Abadi, 2003; Brickell / Camenisch / Chen, 2004.

[532] Eckert, IT-Sicherheit, 2004, S. 2ff.

tem.

Da ein wesentlicher Bestimmungsfaktor des UC die Integration und Vernetzung vorher geschlossener IT-Systeme ist, sind offene Systeme charakteristisch für die zukünftige Entwicklung des UC.

7.2.2.2 Interaktion und Kommunikation im Ubiquitous Computing

Die Charakterisierung des UC durch offene Systeme bedeutet aus technischer Sicht die hochgradige, oft drahtlose Vernetzung einer bisher unbekannten Vielzahl von Geräten und ein enormes Daten- und Kommunikationsaufkommen.

Kommunikationsvorgänge im UC können grob in zwei Kategorien unterteilt werden, einerseits lokal, d.h. in und mit der physischen Umgebung des Nutzers, und andererseits Kommunikation mit entfernten Systemen, z.B. über das Internet. Einen abstrakten Überblick über diese möglichen Kommunikationswege zeigt Abbildung 30, in der aus Gründen der Übersichtlichkeit nur wenige Interaktionsvorgänge dargestellt sind. In der Realität könnten viele derartige Vorgänge parallel ablaufen, wobei jede Interaktion wiederum gleichzeitig auf verschiedenen Informationskanälen ablaufen kann, die mittels unterschiedlicher Basistechnologien[533] implementiert sein können.[534]

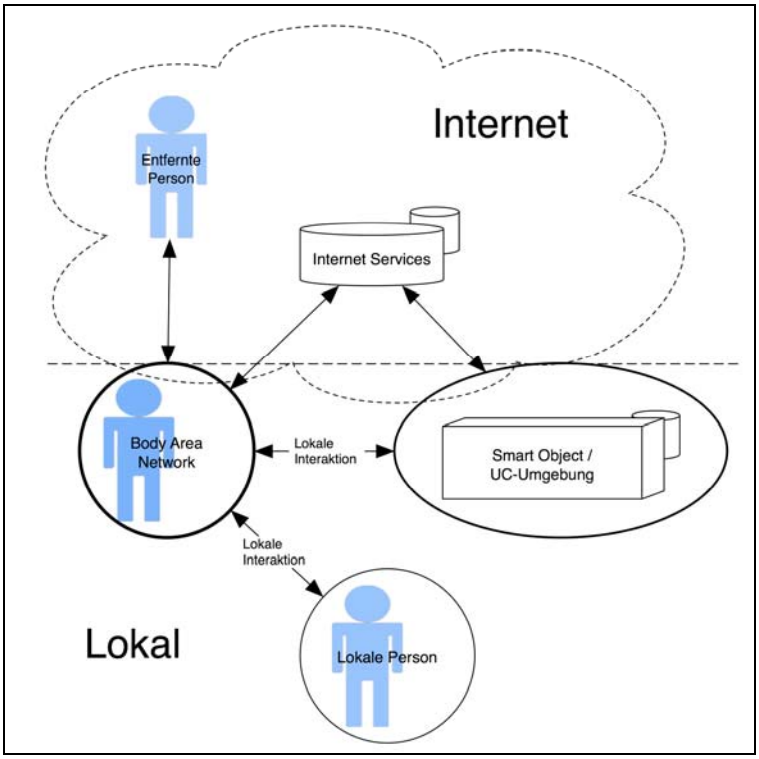


Abbildung 30: Interaktion und Kommunikation im UC

[533] Vgl. Kapitel 1.

[534] Z.B. mittels RFID und Bluetooth, wie im später diskutierten Elope-System: Pering et al., CACM 48 (9), September 2005, S. 53–59.

In der linken Bildmitte steht das Individuum, das von einer „Wolke“ kleiner Geräte umgeben wird, seinem Body-Area-Network (BAN) – oder, oft mit etwas größerer Reichweite gedacht, seinem Personal-Area Network (PAN). Dieses persönliche und stets mitgeführte Netz kann neben größeren Geräten wie einem heutigen Mobiltelefon oder PDA auch diverse kleine in Kleidung und Körper integrierte RFID-Tags und Sensoren enthalten.

Mit fortschreitender Entwicklung des UC werden voraussichtlich zunehmende Anteile des PAN über eine Vielfalt von Access-Technologien (z.B. Bluetooth, WLAN, MAN) direkt mit dem Internet verbunden sein, möglicherweise stets direkt aus der Ferne adressierbar über MIPv6. Das Individuum kann somit über sein PAN Informationen und Services aus dem Internet nutzen oder mit anderen Menschen über das Internet kommunizieren.

Wie bereits heutzutage, zum Beispiel beim Austausch von Daten zwischen Mobiltelefonen und PDAs, so kann auch zwischen den PANs verschiedener Individuuen lokale Kommunikation stattfinden, sei es zum Datenaustausch oder zum gemeinsamen Nutzen einer besseren Internetanbindung (unten im Bild dargestellt).

Eine zentrale neue Komponente ist die Interaktion des Individuums mit einer adaptiven, „intelligenten“ Umgebung, etwa in der Form von einzelnen „Smart Objects“ oder ganzen Räumen im Sinne der „Ambient Intelligence“ (AmI), was in der rechten Bildmitte abgebildet ist. Das Auslesen von am Körper getragenen RFID-Tags durch eine Reader-Umgebung ist ein Vorläufer dieser Interaktion mit einem UC-System der Zukunft – das natürlich ebenfalls RFID benutzen kann, kombiniert mit anderer Sensortechnik.

Diese adaptive Umgebung wird ihrerseits meist mit dem Internet verbunden sein, um externe Datenquellen und Services in ihre Dienstbereitstellung zu integrieren, vgl. dazu Abbildung 2.

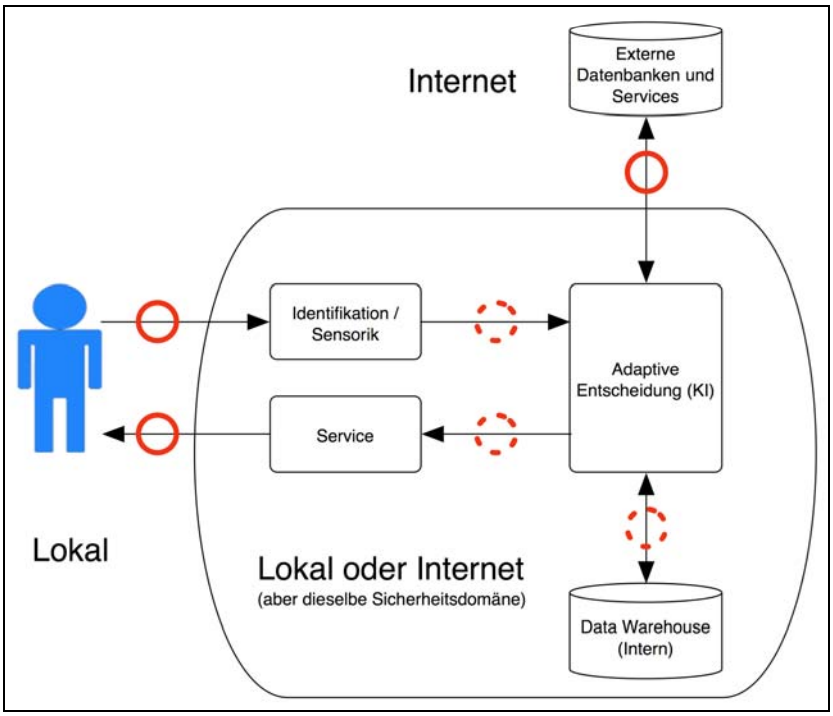


Abbildung 31: Adaptives UC-System (Smart Object oder Intelligente Umgebung)

Natürlich können auch Komponenten des adaptiven UC-Systems selbst – etwa die zur Entscheidungsfindung benutzte interne Datenbank oder ein Data Warehouse – aus dem lokalen System ausgelagert und über das Internet angesprochen werden. Dann werden auch die gestrichelten roten Kreise als Markierung für zu sichernde, lokale oder entfernte Kommunikation relevant, die aber den Vorteil besitzt, in einer einheitlichen Sicherheits- oder Managementdomäne, z.B. der des Betreibers, abzulaufen, weshalb wir sie hier nicht gesondert thematisieren. Auch wenn die Anwendungsszenarien und Technologien von UC zahlreich und unüberschaubar sind, lassen sich somit, basierend auf der vorausgegangenen Systembeschreibung, zwei wesentliche Angriffsrichtungen auf UC-Systeme feststellen: die lokale Interaktion, sowie die Kommunikation mit korrespondierenden Hintergrundsystemen im Internet, siehe Abbildung 32. Diese Unterteilung benutzen wir als Hauptgliederung für die weiteren Abschnitte zur Sicherheit.

Einen Einblick in die Vielfalt möglicher Sicherheitsprobleme im UC geben die Szenarien in Kapitel 4.[535] Um diese Probleme besser fassen zu können, betrachten wir im nächsten Kap. 7.2.2.3 diejenigen Eigenschaften von Interaktion und Kommunikation, die besonders schützenswert sind, d.h. allgemeine Ziele von Informationssicherheit.

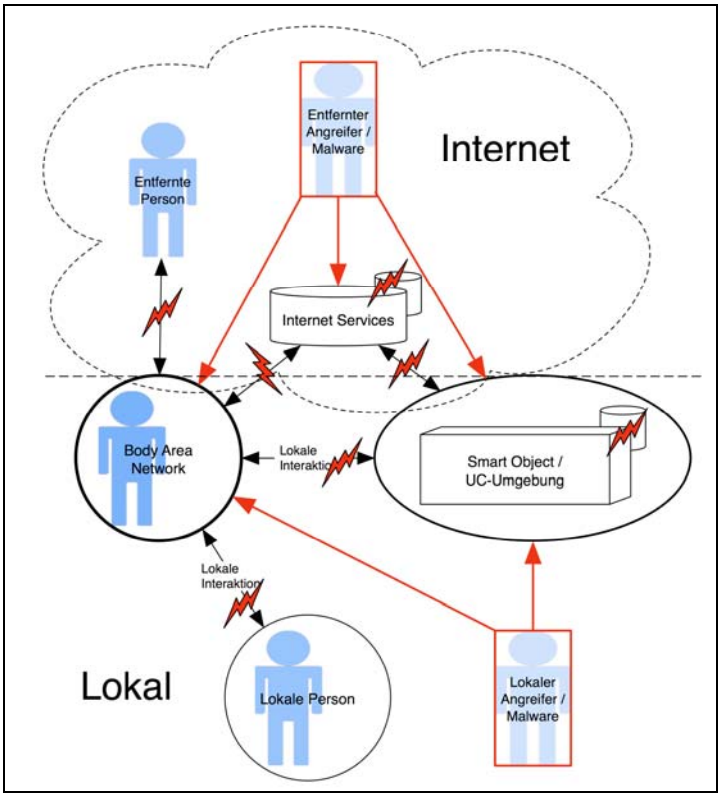


Abbildung 32: Mögliche Angriffswege im UC

[535] Andere sogenannte „Dark Scenarios“ bietet das EU-Projekt SWAMI im Deliverable D2, 2006: http://swami.jrc.es/pages/index.htm (17.03.2006).

7.2.2.3 Ziele von Informationssicherheit

Information als abstraktes Gut kann durch verschiedene konkrete Datenobjekte wie z.B. Daten im RAM, Festplattenblöcke oder IP-Pakete repräsentiert sein. Somit ist auch die Absicherung eines zugehörigen Datenobjekts notwendig, aber nicht ausreichend, denn alle möglichen korrespondierenden Datenobjekte und Informationskanäle müssen geschützt werden. Es genügt zum Beispiel nicht, die Datenpakete einer Informationsübertragung zu verschlüsseln, um ein Mitlesen zu verhindern; es muss auch sichergestellt werden, dass die Information auch, z.B. auf einem entfernten Server als Festplattenblock im Dateisystem, vor unbefugtem Zugriff geschützt bleibt.

Erweitert man dies um eine wichtige Anforderung zum Schutz der Privatsphäre, dass nämlich eine zu schützende Information auch nicht indirekt aus anderen, nur scheinbar irrelevanten Daten abgeleitet oder mit hoher Wahrscheinlichkeit erschlossen werden kann,[536] so wird die – *per definitionem* bestehende – Schwierigkeit offenbar, in UC-Umgebungen mit ihrem hohen Grad an Personalisierung, Kontextbezogenheit und Adaptivität Informationssicherheit und informationelle Selbstbestimmung zu etablieren.

Im Folgenden geben wir einige zentrale Ziele von Informationssicherheit an, die genauso wie in klassischen Netzen auch im UC wichtig sind.[537]

7.2.2.3.1 Vertraulichkeit

Vertraulichkeit kann neben der Geheimhaltung der eigentlichen Kommunikationsinhalte ebenfalls die Anonymität der beteiligten Parteien beinhalten, sowie als weiteren Aspekt, der durch UC stark eingeschränkt werden kann, auch die Vertraulichkeit des Aufenthaltsortes einer Person.

7.2.2.3.1.1 Vertraulichkeit der Kommunikationsinhalte

Werden Informationen in Form von Daten in einem Netzwerk übertragen, so sollen Unbefugte sie nicht abhören können. Insbesondere in drahtlosen Netzen, wie sie im UC verstärkt an Bedeutung gewinnen, ist diese Anforderung sehr wichtig, da ein Abhören leicht und vor allem unauffällig aus der Entfernung stattfinden kann, wie es bereits heutzutage oft bei WLAN praktiziert wird.

Zum Aspekt der Vertraulichkeit gehört auch die Identifizierung, Authentifizierung und Autorisierung von Kommunikationspartnern, denn wenn eine Nachricht mit jemandem verschlüsselt ausgetauscht wird, der sich fälschlich als legitimer Gesprächspartner ausgibt, ist die Vertraulichkeit nicht mehr gegeben.

Ein Beispiel ist das Identifizieren von Gegenständen, die mit RFID-Tags versehen sind und die von Menschen mitgeführt werden. Wenn RFID-Reader in einem Geschäft die Tags in der

[536] Beispiele hierfür sind Verbindungsdaten (für Traffic Analysis), Logfiles auf Servern, GPS Track Logs, Unterschiede im Stromverbrauch von Geräten (Differential Power Analysis) und in der Dauer einer Programmausführung (Timing Analysis).

[537] Überblick zu Zielen von IT-Sicherheit z.B. Stallings, 2002; Eckert, 2004, S. 6ff.; Bless et al., 2005, S. 19f.

Kleidung der Kunden etwa zum Zwecke der Stilberatung auslesen wollen, so sollte geklärt werden, ob der Besitzer dies wirklich wünscht: Gewährt er den fremden RFID-Readern Zugriff auf die eigenen Daten, die ihn auch potentiell identifizieren können? Wie unterscheidet man dabei die Reader des Geschäfts von denen Dritter?

Das zentrale Mittel, um Vertraulichkeit von Inhalten und Authentifikation zu gewährleisten, ist der Einsatz von Kryptographie, was ihre Bedeutung auch für das UC unterstreicht.

In geschlossenen Systemen sind Identifizierung, Authentifizierung und Autorisierung mit klassischen, meist zentralen Methoden[538] relativ leicht zu bewerkstelligen, doch diese Verfahren eignen sich nur wenig für den Einsatz in globalen, offenen Systemen, die bei spontaner lokaler Interaktion möglicherweise keinen garantierten Zugang zu zentralen Servern besitzen, die diese Funktionen gewährleisten könnten.

7.2.2.3.1.2 Vertraulichkeit der Identität (Anonymität)

Anonymität im Sinne der Vertraulichkeit der Identität eines Nutzers kann einerseits gegenüber Dritten gefordert werden, die weder Nutzer noch Dienstanbieter in einem UC-System sind, andererseits auch zwischen den Teilnehmern selbst.

Nicht bei jeder Interaktion im UC sollte die Preisgabe der eigenen Identität vonnöten sein. Dies könnte aber in einen Gegensatz zu einer möglichen Forderung nach vertraulicher Kommunikation und Zugriffskontrolle geraten, bei der, wie oben beschrieben, Identifizierung, Authentifizierung und Autorisierung von Kommunikationspartnern wichtig sein können – andernfalls kann es geschehen, dass man zwar verschlüsselt, aber mit der falschen Partei kommuniziert.[539]

Auch wenn bei dem technischen Kommunikationsvorgang auf der Anwendungsschicht keine Identität preisgegeben werden sollte, so können Protokolle auf niedrigen Schichten des Kommunikationsmodells ihrerseits globale, möglicherweise personenbeziehbare Identifikatoren wie z.B. MAC-Adressen einsetzen. Auf diesen in doppeltem Sinne „vielschichtigen“ Aspekt von Anonymität, der besonders den lokalen Anteil von UC-Systemen aber z.B. auch Mobile IP betrifft, gehen wir im Kap. 7.2.3.2.6.1 zu RFID noch näher ein. Weitere Beispiele für dieses Problem sind Geräteadressen in Bluetooth und WLAN, Identifikatoren zur Kollisionsvermeidung bei RFID, sowie die Möglichkeit, die individuellen Eigenschaften eines Gerätes bei der Funkkommunikation als stellvertretenden „Fingerabdruck“ zu benutzen.

Ferner ist es ggf. auch möglich, sogar im Falle von protokollimmanenter Anonymität aus dem Kontext der Kommunikation (etwa Ort, Zeit, Auslöser) auf den Kommunikationspartner zu schließen. Daher sollte auch auf die Vertraulichkeit dieser Daten geachtet werden.[540]

---

[538] Zum Beispiel zentrale Authentifizierungsserver in einem Firmennetzwerk.

[539] Auch beim Einsatz von verschiedenen Pseudonymen könnte die Forderung nach Authentifizierung ihre Verknüpfbarkeit bewirken.

[540] Noch problematischer und mit UC kaum vereinbar ist das Sicherheitsziel der Unbeobachtkarkeit (unobservability).

7.2.2.3.1.3 Vertraulichkeit des Aufenthaltsortes (Location Privacy)

Die Vertraulichkeit seines Aufenthaltsortes kann ein legitimes Ziel eines jeden Individuums sein. Manche UC-Systeme erfordern zum regulären Betrieb Informationen über den Ort eines Nutzers. So stellt man bei der Nutzung von ortsbasierten Diensten (Location-based Services) dem Dienstanbieter Informationen zum eigenen Aufenthaltsort bewusst zur Verfügung. Doch in vielen anderen Fällen ist die Ortsinformation, die der Betreiber gewinnt, nur ein Nebenprodukt, das von ihm oder Dritten, irregulär, d.h. insbesondere ohne bewusstes Einverständnis des Betroffenen, verwendet werden kann. GPS und die verschiedenen Kommunikationstechnologien des UC, so z.B. die Kommunikation per Funk (GSM, WLAN, RFID) oder Ultraschall, sowie der zunehmende Einsatz von Kameras und Sensornetzen werden das Feststellen des Aufenthaltsortes einer Person mit zunehmender Genauigkeit ermöglichen, vor allem, wenn mehrere Verfahren kombiniert zum Einsatz kommen. Die Vertraulichkeit des Aufenthaltsortes ist insbesondere dann betroffen, wenn der Nutzer die Preisgabe desselben nicht abstellen kann, ohne gleichzeitig eine gewünschte Funktionalität ebenfalls zu deaktivieren. So lässt sich z.B. die Information, in welcher Funkzelle sich ein Mobiltelefon befindet, derzeit nur unterdrücken, indem das Gerät abgeschaltet wird. Bedenklicher ist, wenn man zur Bewahrung der Vertraulichkeit seines Aufenthaltsortes ganze Areale meiden muss, etwa kameraüberwachte öffentliche Bereiche. Dieses Problem wird sich im UC verschärfen, ohne dass sich befriedigende Lösungen auch nur abzeichnen.

7.2.2.3.2 Integrität und Authentizität

Selbst wenn die Kommunikation bereits vor dem Abhören durch Dritte geschützt ist, muss gewährleistet werden, dass die übertragenen Daten nicht mutwillig oder zufällig verändert werden oder dass, wenn dies geschieht, diese Veränderung nicht unbemerkt bleibt (Integrität). Authentizität eines Kommunikationspartners bedeutet den erfolgreichen Nachweis, dass seine angegebene Identität korrekt ist, er also wirklich derjenige ist, der er vorgibt zu sein. Authentizität einer Nachricht besagt, dass sie auch wirklich vom Absender stammt.

Wichtige Mittel zur Gewährleistung von Integrität und Authentizität von Nachrichten sind kryptographische Hashfunktionen. Um verhindern zu können, dass Nachrichten einfach von einem Angreifer kopiert und zu anderer Zeit wiederverwendet werden können, verwendet man in kryptographischen Protokollen oft einmalige Zufallswerte („Nonces“). Dies setzt neben den kryptographischen Funktionen auch gute Pseudozufallszahlengeneratoren (PRNGs) auf den Geräten des UC voraus, was einen weiteren Kostenfaktor darstellt.

7.2.2.3.3 Verfügbarkeit

Eine generelle Voraussetzung für Informationssicherheit[541] ist das korrekte Funktionieren

[541] Eckert, IT-Sicherheit, 2004, S. 2ff.: „Die Informationssicherheit ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder –gewinnung führen.“

eines technischen IT-Systems, die Funktionssicherheit.[542] Zusammen mit Verfügbarkeit und Zuverlässigkeit (Reliability) kann man Funktionssicherheit als Aspekt von Verlässlichkeit (Dependability) auffassen. Andere Autoren ordnen die Verfügbarkeit für autorisierte Nutzer eher als Schutzziel der Informationssicherheit ein.[543] Diese alternative Einteilung wird hier übernommen, wobei besonders die Verfügbarkeit eines Systems auch angesichts eines Angreifers im Vordergrund steht.

Die Verfügbarkeit eines in einem Netzwerk vorhandenen Systems oder Dienstes hat somit zum Ziel, dass authentifizierte und autorisierte Nutzer nicht durch einen Angriff von einer Nutzung abgehalten werden können.

Sogenannte Denial-of-Service (DoS)-Angriffe[544], die auf die Verfügbarkeit von Diensten und Ressourcen zielen, können prinzipiell auf verschiedenen Schichten der Kommunikation durchgeführt werden (z.B. physikalisch durch Störung des Funks oder auf Anwendungsschicht durch zahllose Verbindungsversuche) und sind aufgrund ihrer relativen Einfachheit oft nur schwer zu verhindern.

7.2.2.4 Informationssicherheit in der Praxis

Die Definition von Schutzzielen als Teil einer Anforderungsanalyse eines Systems und der Entwurf von Lösungen zu ihrer Umsetzung ist nicht ausreichend. Bei der praktischen Umsetzung gibt es einige besonders zentrale Faktoren, die auf die Sicherheit eines konkreten IT-Systems einwirken und auch im UC entscheidend werden:

1. Sind auf den beteiligten Geräten kryptographische Verfahren gut einsetzbar, die zur Zeit als sicher gelten können?[545] Diese Verfahren bilden als „Bausteine“ die notwendige Grundlage für Protokolle, die die Einhaltung der Ziele von Informationssicherheit (siehe Kap. 7.2.2.3) gewährleisten sollen.
2. Lösung des Schlüsselmanagement-Problems (besonders Skalierbarkeit): Kryptographie benötigt hinreichend starke Schlüssel. Wie werden diese sicher verteilt, gespeichert und geändert?
3. Sicherheitsbewusstes Design von Systemen, insbesondere Protokollen: Auch mit sicheren Bausteinen lässt sich ein unsicheres System bauen.
4. Korrekte Implementierung: Durch Programmierfehler entstehen die meisten praktisch ausnutzbaren Sicherheitslücken.

---

[542] Ibid.: ‚Unter Funktionssicherheit eines Systems versteht man die Eigenschaft, dass die realisierte „Ist-Funktionalität“ der Komponenten mit der spezifizierten „Soll-Funktionalität“ übereinstimmt. Ein funktionssicheres System nimmt keine funktional unzulässigen Zustände an.’

[543] Gegenüberstellung z.B. in Shirey, RFC 2828, 2000. Siehe auch Eckert, op. cit.; ISO 7498-2, 1989.

[544] Überblick und Erkennungsmethoden bei Carl et al., 2006.

[545] Ein grundlegendes Problem ist, dass sich die Einschätzung der Sicherheit kryptographischer Verfahren schnell ändern kann. Für Bemühungen um die Entwicklung neuer kryptographischer Hashfunktionen siehe z.B. Burr, 2006.

5. Usability: Mit wieviel Aufwand ist die sichere praktische Handhabung des Systems verbunden?

6. Informierte und verantwortungsbewusste Nutzer sowie die Notwendigkeit klar definierter Prozesse: Überforderte, unwillige oder uninformierte Nutzer – inklusive der Administratoren – können sehr gravierende Sicherheitslücken schaffen, genauso wie unklare Zuständigkeiten und Prozesse.[546]

Kryptographie (z.B. kryptographische Hashfunktionen, symmetrische Verschlüsselungsverfahren wie AES oder asymmetrische wie RSA) ist das Hauptwerkzeug, um Informationssicherheit sicherzustellen, und damit auch, um sichere und verlässliche technische Lösungen für die informationelle Selbstbestimmung im UC umzusetzen.

Aus der Verwendung von Kryptographie ergibt sich das grundlegende Problem des Schlüsselmanagements: Wie kann sichergestellt werden, dass nur autorisierte Kommunikationspartner in den Besitz des Schlüssels gelangen (im symmetrischen Fall), bzw., dass der öffentliche Schlüssel eines Kommunikationspartners auch wirklich zu ihm gehört (asymmetrischer Fall)?

Ansätze aus klassischen Netzen wie z.B. eine zentrale Instanz zum Schlüsselmanagement sind in vielen UC-Szenarien mit spontaner Interaktion nicht - oder nur mit unvertretbar hohem technischen und organisatorischen Aufwand - umsetzbar. Eine wichtige offene Frage ist, wie gut entsprechende Verfahren aus dem Bereich der Ad-hoc- und P2P-Netze skalieren und in welchen Anwendungsbereichen sie z.B. auf RFID übertragbar sind. Allein das Problem, eine PIN für einen RFID-Tag[547] oder eine einfache Form der Zugriffskontrolle sicher zu verteilen und für den Verbraucher änderbar zu gestalten, ist komplex, da dazu neben dem Transfer des Tags ein sicherer, d.h. insbesondere authentifizierter und verschlüsselter Informationskanal zwischen Anbieter und Endkunde notwendig ist.[548]

In manchen klassischen Beschreibungen von IT-Systemen als rein technischen Systemen[549] sind die Nutzer nur implizit berücksichtigt, was sich zwar als nützliche Abgrenzung in der Theorie, als Grenze der Betrachtung in der Praxis aber leider oft als unzureichend erweist.[550] Diesen Aspekt gilt es bei allen möglichen Lösungen, die oft noch nicht über ein theoretisches

---

[546] Hier setzen in Organisationen z.B. Informationssicherheits-Managementsysteme (ISMS) an, die zur Umsetzung von Spezifikationen wie BS7799 dienen (international normiert als ISO/IEC 27001:2005). Für eine Abgrenzung und Vergleich zum deutschen IT-Grundschutz vgl.: http://www.bsi.de/gshb/deutsch/hilfmi/bs7799.htm (13.03.2006).

[547] Z.B. ein in bestimmten Standards vorgesehenes Kill-Passwort, das Tags deaktivieren soll (Kap. 7.2.3.2.4.2).

[548] Dieses PIN-Verteilungsproblem für RFID – als Spezialfall eines allgemeinen Schlüsselmanagement-Problems – wird z.B. auch bei Juels, Survey, 2005, S. 12, als wichtiges offenes Forschungsgebiet genannt. Ähnlich Molnar / Soppera / Wagner, Privacy for RFID Through Trusted Computing, 2005.

[549] Beispielsweise Eckert, IT-Sicherheit, 2004, S. 2: „Ein IT-System ist ein geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen."

[550] Siehe auch Anderson, 2001, S. 8-9.

technisches Design hinausgekommen sind, als fundamentales praktisches Problem zu berücksichtigen.

Nach diesen allgemeinen Betrachtungen richten wir den Blick zunächst auf Lösungen für Informationssicherheit in lokalen UC-Systemen, die in direkter Interaktion mit den Nutzern stehen, um dann in einem späteren Abschnitt Lösungen für gekoppelte entfernte Systeme zu betrachten.

7.2.3 Informationssicherheit in lokalen UC-Systemen

Die sichtbaren technischen Neuerungen wie z.B. RFID-Tags und -Reader zeigen sich dem Nutzer in der Interaktion und Kommunikation mit lokalen UC-Systemen oder präziser dem lokalen Teilsystem einer UC-Umgebung, wie im vorherigen Kap. 7.2.2.2 zur Kommunikation im UC beschrieben.

Wie in AP1 dargestellt, können RFID-Systeme als annähernd prototypisch für allgemeines UC angesehen werden. Neben RFID werden im allgemeinen UC auch Netzwerke aus Sensoren[551] und Aktoren[552] bedeutsam, die in „Smart Environments“ eingebettet sind, ferner von Individuen mitgeführte „Personal“ und „Body Area Networks“, Ad-hoc-Netzwerke und automatische Interaktionen zwischen Geräten und Objekten unter dem Schlagwort vom „Internet of Things“. Die Probleme, die bei RFID in der Sicherung von Daten auf den Tags und der Tag-Reader-Kommunikation auftreten, sind ein wichtiger Spezialfall des allgemeinen Problems von Sicherheit und Datenschutz in lokalen UC-Systemen und werden in den folgenden Betrachtungen einen breiten Raum einnehmen.[553]

7.2.3.1 Ein Lösungsideal: Geräte im UC als „Wiederauferstehende Entlein“ (Resurrecting Ducklings)

Vor der Diskussion konkreter Lösungsansätze für die Umsetzung von Informationssicherheit in lokalen Systemen sei an dieser Stelle ein abstraktes Anforderungsmodell vorgestellt, das gewissermaßen aus einem idealistischen Blickwinkel beschreibt, wie das Verhältnis zwischen Nutzern und Geräten im UC gestaltet sein müsste, um Sicherheit und informationelle Selbstbestimmung zu wahren.[554]

Ausgangspunkt ist eine ideale Beschreibung des Vorganges, wie ein Computer an einen Besitzer oder dessen Stellvertreter wie einen mitgeführten ID-Manager durch ein Passwort gebunden werden sollte, damit eine sichere, vorübergehende Assoziierung (Secure Transient Association) von Mensch und Gerät gewährleistet ist. Das „Resurrecting Duckling“ Mo-

[551] Z.B. Bewegungsmelder, Temperaturfühler, aber auch netzfähige Mikrophone und Kameras.

[552] Aktoren (auch Aktuatoren genannt) sind Geräte, die über ein Netzwerk aus der Ferne kontrollierbare Bewegungen und Aktionen auslösen können.

[553] Ein EU-Projekt, dass sich mit lokaler Sicherheit in allgemeinen UC-Systemen, z.B. sicherer Dienstvermittlung beschäftigt, ist UBISEC: http://jerry.c-lab.de/ubisec/ (17.03.2006).

[554] Stajano, Security for Ubiquitous Computing, 2002, S. 88ff.

dell für eine Security Policy[555] ist ursprünglich von der Prägung frisch geschlüpfter Graugänse auf die Muttergans beeinflusst:[556]

- Prinzip der zwei Zustände, (Two State Principle): Ein Gerät kennt genau zwei Zustände, es ist entweder prägbar (imprintable) oder bereits von einer „Mutter" geprägt (imprinted).
- Prägungs-Prinzip (Imprinting Principle): Ein fabrikneues Gerät, das aus seiner Verpackung genommen wird, erkennt als Besitzer oder „Mutter" das erste Gerät oder Wesen an, das ihm über einen sicheren, d.h. vertraulichen und integren Kanal[557] einen geheimen Schlüssel übermittelt.
- Todesprinzip (Death Principle): Solange das Gerät geprägt ist, folgt es nur den Anweisungen des Muttergeräts, mit dem es dank des Schlüssels auch vertraulich kommuniziert. Allein die Mutter kann auch dem Gerät befehlen, wieder in seinen ursprünglichen, prägbaren Zustand zurückzukehren, was auch nach Ablauf einer bestimmten Zeit oder Erfüllung einer Transaktion geschehen kann. Beim Tod vergisst das Gerät alle bisherigen Daten und den geheimen Schlüssel, kehrt in den fabrikneuen Zustand zurück und wartet auf eine neue „Mutter", die ihm einen Schlüssel zur festen Bindung zusendet (Resurrection: Wiederauferstehung, allerdings mit neuer „Seele").
- Assassinierungs-Prinzip (Assassination Principle): Das Gerät muss so konstruiert sein, dass es für einen Angreifer einen zu hohen Aufwand verursachen würde, den „Tod" des Gerätes – in obigem Sinne, nicht die physische Zerstörung – unautorisiert herbeizuführen; somit ist beim Gerät ein gewisser Schutz vor physischer Manipulation[558] notwendig.

Gerade angesichts möglicherweise nicht vorhandener oder unerreichbarer Authentifizierungs-Server in allgemeinen UC-Szenarien liegt ein besonderer Reiz des Resurrecting Duckling-Models in seinem Verzicht auf Identifikation zwecks Authentifizierung: Es ist egal, wie die Mutter heißt, Hauptsache, sie hat den korrekten Schlüssel, den das Gerät seit seiner Geburt kennt.[559]

[555] "A security policy model is a succinct statement of the protection properties which a system, or generic type of system, must have." Ibid., S. 82. Hier zu unterscheiden von Dokumenten aus dem Sicherheitsmanagement.

[556] Die Bezeichnung Entlein („Duckling") entstammt einem Übersetzungsproblem eines Buches von Konrad Lorenz, wurde von Stajano später aber beibehalten.

[557] Stajano und Anderson empfehlen physischen Kontakt für einen sicheren Kanal im UC (ibid., S. 90).

[558] Überblick zu „Tamper-Resistance" z.B. bei Anderson, 2001, S. 277ff.

[559] Stajano spricht von anonymer Authentifizierung. Komplexere Formen von Authentifzierung mit unterschiedlichem Grad an Anonymität gegenüber Kommunikationspartnern und vertrauenswürdigen Dritten z.B. bei Chaum, 1985; Abadi, 2003; Brickell / Camenisch / Chen, 2004.

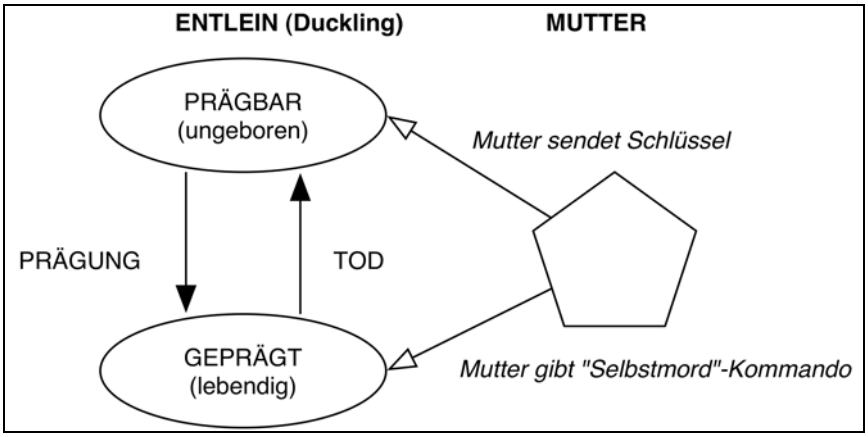


Abbildung 33: Zwei Zustände des „Duckling" (Stajano, 2002)

Ein anschauliches Beispiel[560] ist die Verwendung von UC in einem Krankenhaus. Angenommen, es gibt dort einen Pool von identischen elektrischen, drahtlosen Thermometern, die Temperaturdaten an den PDA eines Arztes senden können. Es ist für den Arzt nicht wichtig, welches Thermometer zum Einsatz kommt, aber sobald es bei einem Patienten ist, so soll der PDA genau dieses Thermometer kontaktieren, und nicht ein anderes in der Nähe. Aus Datenschutzgründen sollte das Thermometer die Daten nach seinem Einsatz beim Patienten „vergessen", also zum Ausgangszustand zurückkehren.

Das „Resurrecting Duckling"-Modell eignet sich zumindest für alle Anwendungen, wo eine sichere, vorübergehende Assoziierung von Entitäten (Menschen, Mutter-Geräten) mit anderen Geräten erfolgen soll. Inwieweit dieses Prinzip zum Beispiel bei gleichberechtigten Ad-hoc–Netzen anwendbar ist, kann nur in der konkreten Anwendung entschieden werden.

Wichtig ist bei einer Implementierung in konkreten Systemen, dass nicht nur einige, sondern alle Prinzipien vollständig erfüllt sind. Insbesondere das „Vergessen" aller alten Daten bei der Rückkehr des Gerätes in den prägbaren Zustand ist ein aus Datenschutzsicht hervorzuhebender Aspekt.

Generell gibt das Modell keinen Hinweis, ob und mit welchen Mitteln die einzelnen Prinzipien umzusetzen sind, insbesondere wenn die kryptographischen Bausteine fehlen. In der Praxis problematisch ist auch die Notwendigkeit eines sicheren Kanals für die Prägung, aber genau hierin offenbart sich das Problem des Schlüsselmanagements. Die Variante, Berührung als solch einen sicheren Kanal zu verwenden, ist sicherlich sehr intuitiv, wird im UC aber nicht immer möglich sein.

Der bleibende Wert eines solchen Modells aber ist auch die klare und einfache Darstellung der Sicherheits- und Datenschutzanforderungen, was bei der Bewertung einer praktischen Umsetzung hilfreich ist.

[560] Ibid., S. 88.

7.2.3.2 Informationssicherheit in RFID-Systemen

Ein zentraler Baustein des UC und des „Internets der Dinge" ist die Technik der Radio-Frequenz-Identifikation (RFID).[561] Wir gehen zunächst auf die Besonderheiten der Datenspeicherung bei RFID und die möglichen Risiken von RFID-Systemen für Informationssicherheit und informationelle Selbstbestimmung ein, bevor wir die technischen Voraussetzungen von RFID für die Umsetzung von Informationssicherheit diskutieren und einen Überblick über Lösungsvorschläge geben.

7.2.3.2.1 Zentrale oder dezentrale Datenhaltung bei RFID

Es gibt zwei gegensätzliche Designmöglichkeiten zur Datenhaltung bei RFID. Einerseits können mit zunehmender Leistungsfähigkeit mehr Daten auf den Tags selbst gespeichert werden, somit lokal und direkt in der Interaktion mit dem Objekt zur Verfügung stehen (Prinzip „Data on Tag").

Andererseits besteht die Kernfunktion von RFID in der reinen Identifikation von Objekten, die eigentlichen Daten zum Objekt können danach aus Hintergrunddatenbanken bezogen werden (Prinzip „Data on Network"). Diese zweite Variante wird insbesondere mit den simplen EPC-Tags (Class 1) verwirklicht, die gerade durch ihre nur einfache Funktionalität als drahtlos auslesbares Nummernschild massenmarkttaugliche Preisregionen erreichen können.

Natürlich bestehen diverse Kombinationsmöglichkeiten zwischen diesen Extremen, deren Wahl in der Praxis vor allem aus den Zwängen der jeweiligen Anwendung und technischen sowie ökonomischen Rahmenbedingungen erfolgt. Die Festlegung eines Designs für die Datenspeicherung hat allerdings direkte Auswirkungen auf Informationssicherheit und, im Falle von privaten Objekten mit Tags, auf die informationelle Selbstbestimmung der Besitzer.

Aus Sicht der Informationssicherheit und praktischen Handhabbarkeit[562] wird oft ein zentralisiertes Modell postuliert, wobei sich die Datenbanken durch ihre Platzierung in leichter kontrollierbaren Netzumgebungen besser schützen, überwachen und bei Softwarebugs schneller mit einem Upgrade versehen lassen. Allerdings hat dieser zentralistische Ansatz durch erfolgreiche Angriffe auf einige zentrale Datenbestände von Datenbrokern[563], Hotels[564], Banken[565] und Kreditkartenunternehmen[566] einiges von seiner scheinbar evidenten Überzeugungskraft eingebüßt – wenn selbst einige Unternehmen der Kreditindustrie ihre großen, zentralen Datenbestände nicht schützen können, so erscheint Skepsis angebracht. In der

---

[561] Grundlegenden Überblick zu Fragen von Sicherheit und informationeller Selbstbestimmung bei RFID bieten: BSI 2004; Langheinrich, 2005; Garfinkel / Juels / Pappu, 2005; Ohkubo et al., 2005; Juels, 2005.

[562] Beispielsweise mit den Kriterien leichte Aktualisierbarkeit und einfacher Zugriff auf die Daten.

[563] Z.B. ChoicePoint und LexisNexis, Heise Newsticker, 06.03.2005, http://www.heise.de/newsticker/meldung/57117 ; ibid., 13.04.2005, Meldung 58523 (13.06.2006).

[564] Ibid., 29.12.2005, Meldung 67824 (13.06.2006).

[565] Ibid., 26.02.2005, Meldung 56836 (13.06.2006).

[566] Ibid., 18.06.2005, Meldung 60767; zu Datendiebstahl bei angeschlossenen Handelsketten siehe z.B. ibid., 14.04.2005, Meldung 58591; 19.04.2005, Meldung 58733 (13.06.2006).

Praxis stellt sich auch das Problem, wie die Daten von einfachen Geräten wie Tags – und auch Sensorknoten – sicher an eine Zentrale übermittelt werden können. Hier besteht viel Spielraum für fehlerhafte Implementierung und Bedienung.

Andererseits ist auch die dezentrale, verteilte Haltung der Daten auf unsicheren Einzelgeräten aus Sicht der Informationssicherheit keine sehr verlockende Perspektive. Hinzu kommt, dass es auch stark davon abhängt, wo die Daten genutzt werden sollen, lokal beim Objekt, oder entfernt z.B. zu Monitoring-Zwecken. Somit ist aus Sicht der Informationssicherheit keine der beiden Designentscheidung ein Königsweg.

Wie sieht es aus der Sicht der informationellen Selbstbestimmung aus? Einerseits gründet sie sich auf Informationssicherheit, andererseits hat sie mächtige Gegenspieler in Profilingtechniken und Data Mining auch von scheinbar belanglosen Informationen, wie beispielsweise Zugriffszeit und –ort auf bestimmte Datensätze. Zumindest was diesen zweiten Aspekt angeht, scheint lokale Datenhaltung in den Tags von Objekten Data Mining schwieriger zu machen.[567]

Was den subjektiven Aspekt der empfundenen „Kontrolle über die eigenen Daten“ betrifft, ist eine lokale Datenspeicherung in Objekten wahrscheinlich von Vorteil. Da der Standard bei EPC-Tags für den Massenmarkt allerdings im Moment eindeutig „Data-on-Network“ bevorzugt, folgt ein kurzer Überblick über die möglichen Risiken solcher Systeme.

7.2.3.2.2 Allgemeine Sicherheitsrisiken für RFID-Systeme

Einige allgemeine Sicherheitsrisiken für RFID-Systeme, die sich auch bei beliebigen Kommunikationssystemen finden, sind:[568]

- Sniffing: Verläuft die Kommunikation zwischen Reader und Tags im Klartext, so können Dritte in Funkreichweite[569] sie passiv mitlesen und somit auch eventuell übertragene Passwörter oder Daten in Erfahrung bringen.
- Spoofing: Ohne angriffssichere Authentifizierungsmaßnahmen kann man Reader mit gefälschten Tags einfach täuschen.[570] Falls eine Zugriffskontrolle auf leistungsfähigeren Tags anhand von Reader-IDs implementiert werden sollte, besteht auch hier die Möglichkeit, eine falsche Identität vorzuspiegeln. Der getäuschte Kommunikationspartner verhält sich ohne weitere Sicherheitsmaßnahmen so, als ob sein Gegenüber echt wäre, vertraut insbesondere übertragenen EPCs, Daten oder Kommandos.

---

[567] Dies muss allerdings nicht in jedem Fall gelten, z.B. nicht in permanent mit RFID-Readern oder zusätzlichen weiteren Techniken überwachten Gebieten.

[568] Teilweise in Anlehnung an Rieback / Crispo / Tanenbaum, IEEE Pervasive Computing, 5(1), 2006, S. 62–69.

[569] Die Sendereichweite von Readern und Tags unterscheidet sich (allein schon wegen der jeweils verfügbaren Energie), da aber Funkempfang in der Praxis von sehr vielen Faktoren und insbesondere von der Empfängerantenne abhängt, sollte keine Sicherheitsmaßnahme allein auf diesem Unterschied basieren.

[570] Ein Beispiel einer Reader-Täuschung bei vorhandener, aber ungenügender Zugriffskontrolle bieten Bono et al., 2005.

- Replay-Angriffe: Ein Angreifer kann nach einem erfolgreichen Sniffing-Angriff die abgehörte Kommunikation speichern und später wieder „abspielen“. Die möglichen Folgen hängen von der Anwendung und Situation ab. Gibt es z.B. keine Sicherheitsmaßnahmen wie Challenge-Response-Verfahren mit jeweils neu und zufällig generierten Challenges, könnte dieses Wiederabspielen einem Angreifer das Vortäuschen einer fremden Identität ermöglichen.
- Denial of Service: Von Störung des Funks bis zu protokollkonformer Überlastung von Readern oder Zerstörung von Tags ergeben sich diverse Möglichkeiten, ein RFID-System am korrekten Funktionieren zu hindern.

Je nach Anwendung, Kontext und Zeitpunkt sind solche Angriffe mehr oder minder wahrscheinlich und folgenschwer; sie könnten auch die physische Sicherheit von Menschen gefährden und sich negativ auf die informationelle Selbstbestimmung von Systemteilnehmern auswirken.

7.2.3.2.3 Spezielle Risiken durch RFID-Tags mit global eindeutigen Identifikationsnummern

Auch wenn wir in diesem Kapitel hauptsächlich die Risiken lokaler UC-Systeme behandeln, berücksichtigen wir in diesem Abschnitt zu global eindeutigen Identifikatoren wie dem Electronic Product Code (EPC) auch gekoppelte Hintergrundsysteme. Im Einklang mit den Visionen der Proponenten des Einsatzes von RFID auf jedem einzelnen Waren-„Objekt“ und besonders auch für Dienstleistungen nach dem Kauf stellen wir uns ein Szenario vor, in dem RFID-Tags mit zugehörigen EPCs auf den meisten Alltagsgegenständen vorhanden oder sogar fest integriert sind. Parallel existiere eine dichte Reader-Infrastruktur verschiedener Betreiber, zum Beispiel in Bekleidungsgeschäften und Smart Homes.

Möchte jemand, in der Terminologie der IT-Sicherheit oft Angreifer oder Widersacher genannt, heimlich in Erfahrung bringen, was eine Person P in ihrem Besitz hat, so könnte er lokal vorgehen, indem er die RFID-Tags der Person direkt ausliest oder z.B. eine legitime Tag-Reader Kommunikation abhört. Möglicherweise gelingt es ihm auch, eine drahtlose WLAN-Kommunikation zwischen Lesegeräten und Backend abzuhören. Diese Form des Angriffs ist lokal. Lösungen zur Sicherung werden im weiteren Verlauf dieses Abschnitts (Kap. 7.2.3) diskutiert.

Ein anderer Angreifer mit demselben Ziel findet ein Abhören und Profiling auf Distanz interessanter oder leichter realisierbar: Er kann Zugang zu Telekommunikationsdaten des Smart Homes von P haben oder Zugriff auf die Logfiles von ONS- oder EPC Information-Servern besitzen (zum EPC-Netzwerk vgl. unten Kap. 7.2.4.2.1). Jedes Mal, wenn die intelligente Hausinfrastruktur Informationen zu einem Objekt und seinem EPC abruft, liest er mit und könnte so mittelfristig einen Großteil des Eigentums von P katalogisieren. Dieser Angriff nutzt gekoppelte Internetsysteme, die einem Zugang oder Aufschluss über lokale Gegebenheiten aus der Ferne eröffnen.

Natürlich sind beide Angriffspfade mit etlichen praktischen Schwierigkeiten behaftet und hängen von sehr vielen Parametern wie z.B. dem Grad der Durchdringung des Alltags mit

RFID und Häufigkeit der Lesevorgänge ab; das Prinzip der miteinander verschränkten lokalen und entfernten Sicherheitsprobleme bei UC wird hier aber bereits bei RFID deutlich.

Analog zum Auslesen von Besitz bestehen in einem solchen Szenario verschiedene Möglichkeiten, den Aufenthaltsort und die Bewegung einer Person P zu verfolgen. Ein US-Patentantrag von IBM aus dem Jahre 2001[571], der als solcher zumindest nicht vollkommen unrealistische Zielsetzungen verfolgen kann, beschreibt eine solche Überwachungsfunktion durch RFID wie folgt:

„A method and system for identifying and tracking persons using RFID-tagged items carried on the persons. Previous purchase records for each person who shops at a retail store are collected by POS terminals and stored in a transaction database. When a person carrying or wearing items having RFID-Tags enters the store or other designated area, a RFID-Tag scanner located therein scans the RFID-Tags on that person and reads the RFID-Tag information. The RFID-Tag information collected from the person is correlated with transaction records stored in the transaction database according to known correlation algorithms. Based on the results of the correlation, the exact identity of the person or certain characteristics about the person can be determined. This information is used to monitor the movement of the person through the store or other areas.“[572] (Abstract)

"In another embodiment, instead of determining the exact identity of the person, some characteristics such as demographic (e.g., age, race, sex, etc.) may be determined based on certain predetermined statistical information. For example, if items that are carried on the person are highly expensive name brands, e.g., Rolex watch, then the person may be classified in the upper-middle class income bracket. In another example, if the items that are carried on the person are "female" items typically associated with women, e.g., a purse, scarf, pantyhose, then the gender can be determined as female.“ (S. 2)

Die Auswirkungen allgegenwärtiger Infrastrukturen von RFID-Readern werden ebenfalls bereits von IBM beschrieben:

"When a person enters a retail store, a shopping mall, an airport, a train station, a train, or any location where a person can roam, a RFID-Tag scanner located therein scans all identifiable RFID-Tags carried on the person..." (S. 3)

"The present invention has wide applicability. For example, the present invention can be used to track and follow a particular crime subject through public areas by tracking the identity, location and time the subject came in contact with others." (S. 3)

Das direkte Tracking der RFID-Tags einer bestimmten Person mag unter bestimmten Umständen wegen geringer Lesereichweiten zu mühsam sein; wenn ein Angreifer aber Zugriff auf Datenbanken mehrerer Betreiber von Lesegeräten oder deren Netzwerkverkehr hat, so lassen sich für P charakteristische Gegenstände oder Cluster von EPCs – wenn auch mit höherer statistischer Unsicherheit – auch aus der Ferne verfolgen.

---

[571] Ausführliche Behandlung in Albrecht / McIntyre, Spy Chips, 2005, S. 32ff.

[572] Hind / Mathewson / Peters, US-Patentantrag (Application Number: 20020165758): „Identification and tracking of persons using RFID-tagged items“, 2001.

Je nach Motiven und Infrastruktur eines Angreifers kann es für ihn auch sehr interessant sein zu beobachten, welche EPCs auf Objekten verschiedener Personen wo und wie oft zusammen ausgelesen werden, um Schlussfolgerungen über mögliche Kontakte abzuleiten.

Als wesentliche Ziele von Angriffen auf die informationelle Selbstbestimmung mithilfe von RFID-Technologie gelten:[573]

- Nicht autorisiertes Erfassen von Besitz.
- Tracking und Identifizieren von Personen.
- Erheben sozialer Strukturen und Kontakte.

Zur Strukturierung der Methoden, die ein Angreifer wählen kann, um ein bestimmtes Ziel Z(i) zu erreichen, kann man sogenannte Angriffsbäume (Attack Trees) verwenden.[574] Um die wesentlichen Angriffsorte (lokale RFID-Kommunikation, Hintergrundsysteme) aufzuzeigen, geben wir hier keinen Baum für einen konkreten Angriff, sondern etwas abstrakter einen Meta-Baum an, der für spezielle Ziele konkretisiert werden kann. Diese Strukturierung kann eine Grundlage für detaillierte Risikoanalysen bilden, die aber genauere Informationen über den speziellen Anwendungskontext und die verwendeten Systeme erfordert.

Deutlich wird die Zweiteilung in lokale (Tag-Reader, lokale Systeme)[575] und entfernte Angriffspfade (ONS, EPC Information Service)[576], die ein Angreifer wählen könnte – abhängig von seinen eigenen Fähigkeiten, den für ihn dabei entstehenden Kosten und natürlich der Eignung des jeweiligen Unterzweiges für das spezielle Angriffsziel Z(i).

Ein weiteres Risiko der Integration von RFID-Tags in langlebige Alltagsgüter ist die Gefahr einer langfristigen Objektverantwortlichkeit: Die Verbindung aus EPC und Identität wird mit zunehmender Nutzungsdauer der Objekte leichter feststellbar, andererseits könnte ein starker Angreifer diese Verbindung bereits aus Datenbanken des Verkäufers ermitteln, selbst wenn Tagdaten und persönliche Daten der Kaufabwicklung getrennt gespeichert sind. Ort und Zeit der Transaktion wären ein guter Kandidat für einen Primärschlüssel.

In Anlehnung an den Begriff „RFID-Shadow“[577] könnte man bei Berücksichtigung von Datenbanksystemen im Hintergrund von einem EPC-Schatten sprechen, den Personen und Institutionen in der virtuellen Welt hinterlassen könnten.[578] Die weiter unten diskutierten Lö-

---

[573] Die Problematik des „Technologiepaternalismus“ und andere Risiken des UC, die nicht primär zur Informationssicherheit gehören, bleiben an dieser Stelle unberücksichtigt.

[574] Siehe Schneier, Attack Trees, 1999.

[575] Detailliert in Spiekermann / Ziekow, 2004.

[576] Siehe Fabian / Günther / Spiekermann, 2005.

[577] Garfinkel / Juels / Pappu, 2005, S. 38.

[578] Nebenbemerkung: Eine neue potentielle Gefährdungsdimension stellt der EPC per se insofern dar, als er langfristig fast alle zum Handel geeigneten physischen Objekte hinreichender Größe erfassen soll. Global eindeutige Seriennummern als mögliche, aber schwer zu quantifizierende Bedrohung der Privatsphäre gibt es in vielen verschiedenen Bereichen, so zum Beispiel auf Banknoten (siehe Kügler, 2005) oder fast unsichtbar auf allen gedruckten Seiten bestimmter Laserdrucker, http://www.eff.org/Privacy/printers/docucolor/ (13.03.2006).

sungsansätze versuchen im Wesentlichen, den Umfang dieses „Schattens“ zu reduzieren oder zumindest geordnete Zugriffsregeln zu etablieren.

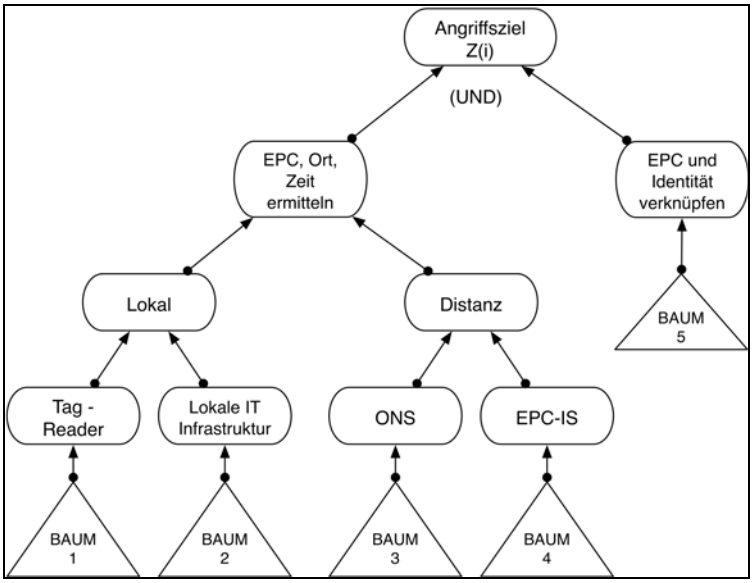


Abbildung 34: (Meta-)Angriffsbaum für RFID- und EPC-Systeme

Vor dem Hintergrund dieser Risiken werden in den folgenden Abschnitten Sicherheitslösungen vorgestellt und diskutiert. Verwendete Kategorien dafür sind Zugriffskontrolle, Sicherung der eigentlichen Kommunikation, Pseudonymisierung und technisch unterstützte organisatorische Verfahren, die nur auf Vertrauen in einen Serviceprovider setzen. Zunächst wird allerdings erörtert, welche Voraussetzungen für solche Lösungen auf den verschiedenen Tag-Klassen bestehen.

7.2.3.2.4 Sicherheitsvoraussetzungen bei RFID-Tags

Aus Sicht der Informationssicherheit und informationellen Selbstbestimmung ist entscheidend, ob und inwieweit Ideale wie der „Resurrecting Duckling“ überhaupt bei RFID praktisch umgesetzt werden können.

Im Allgemeinen geht man davon aus, dass RFID-Reader an eine feste Infrastruktur gekoppelt sind und stärkere Leistungsdaten (Speicher, Prozessor, Energie) besitzen als die kleinen RFID-Tags.[579]

Zentrale Fragen sind also: Wie stark und wie bewährt ist die Kryptographie[580], die auf RFID-Tags überhaupt eingesetzt werden kann? Welche Verfahren arbeiten unter diesen stark ein-

[579] Dort allerdings, wo RFID-Reader (eventuell mobile) drahtlose Sensoren im Sinne der Sensornetzforschung sind, kann diese Annahme durchaus problematisch sein.

[580] Einführung und Überblick zur Verwendung von Kryptographie in „klassischen“ Netzwerkprotokollen bei Stallings, 2002; Menezes / Oorschot / Vanstone, 1997; Bless et al., 2005. Fundamentalwerk zur Kryptographie: Goldreich, 2003/2004.

schränkenden Bedingungen und können noch als sicher erachtet werden?[581] Und drittens, stellt sich die Frage nach der Bewertung mangelnder Sicherheitsvoraussetzungen. Falls und solange Tags mit guter Sicherheitsfunktionalität auf absehbare Zeit zu teuer für den Massenmarkt sind, sollte man nicht besser vom Einsatz von RFID auf Einzelprodukten nach dem Kauf absehen?

7.2.3.2.4.1 Einfache RFID-Tags

Eine zwar grobe, aber nützliche Kategorisierung von RFID-Tags orientiert sich an der geschätzten Stärke der auf ihnen implementierbaren Kryptographie. Aus Sicht der Informationssicherheit einfache Tags[582] sind solche, die über keine Standard-Kryptofunktionalität verfügen, wie z.B. bewährte Verschlüsselungsverfahren und kryptographische Hashfunktionen, sowie Pseudozufallsgeneratoren (PRNG).

Zu den einfachen Tags gehören aufgrund ihres bisher geringeren Preises vor allem die für den Massenmarkt vorgesehenen EPC-Tags für Einzelprodukte („Item-level"), die wir im anschließenden Abschnitt behandeln.

Aus Sicht der Informationssicherheit ist eine unverschlüsselte Kommunikation über eine Funkschnittstelle, die zudem auch noch ohne Authentifikation erfolgt, vollkommen indiskutabel, es sei denn, der Einsatz beschränkt sich auf ein erwiesenermaßen isoliertes, geschlossenes System. Auch wenn die Sensibilität der übertragenen Daten eventuell von vielen Beteiligten zu einem bestimmten Zeitpunkt für gering erachtet wird, so ist diese Einschätzung nicht absolut und kann sich je nach Zeitpunkt, Kontext und Ausmaß der möglichen Datenaggregierung ändern. Dann wären aber diese einfachen Tags möglicherweise bereits in einem solchen Maßstab im Umlauf, dass ein Austausch oder nachträgliches Aufrüsten mit Sicherheitsfunktionalität sehr aufwändig wäre.

Das einzige Argument für diese ungeschützten Tags ist ein – ohne Berücksichtigung etwaiger Risiken und Folgekosten wahrscheinlich zu kurz gedachtes – unilateral-ökonomisches: Sie sind bisher am günstigsten in der Produktion. Auch hier, wie im Bereich der klassischen IT, wird man mit Bruce Schneier fragen müssen: Wer wird die Kosten der unzureichenden Sicherheit tragen?[583]

7.2.3.2.4.2 Beispiel: EPC-Tags, Class-1

RFID-Tags, die den Standards EPCglobal Class-0 und EPCglobal Class-1 (Generation 1)

---

[581] Selbst bei theoretisch geeigneten Verfahren besteht in der Praxis immer die Gefahr von Side-Channel-Attacks, die z.B. mittels von genauer Analyse von Timing und Energieverbrauch scheinbar sichere Systeme kompromittieren können. Siehe Anderson, 2001, S. 305ff.; speziell zu RFID EETimes, „Cellphone could crack RFID tags, says cryptographer", 14.02.2006: http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=180201688 (13.03.2006).

[582] In Anlehnung an Juels, 2005, S.7, wo diese Tags „basic" genannt werden. Ohkubo et al., 2005, sprechen von „normal tags".

[583] Bruce Schneier auf der RSA Security Conference 2005, zitiert nach und übersetzt durch Heise Newsticker: http://www.heise.de/newsticker/meldung/65128 (20.10.2005): „Die Kosten für Sicherheitslücken werden nicht von denen getragen, die darauf einen direkten Einfluss haben, sondern vielmehr von denjenigen, die unter den Mängeln leiden."

entsprechen, enthalten keine eigentliche Schutzfunktionalität. Tags nach dem EPCglobal Class-1 (Generation 2) Standard[584] sehen ein 32 Bit langes „Kill-Passwort“[585] vor, das den permanenten Deaktivierungsvorgang (kill) absichern soll.

Ebenso kann ein optionales 32-Bit sogenanntes „Zugriffspasswort“ (access) spezifiziert werden, das ein Reader übermitteln muss, um den Tag in einen sogenannten „Secure State“ zu versetzen; dann sind alle Kommandos inklusive *lock* ausführbar, mit dem Passwörter und Speicherabschnitte permanent schreibgeschützt werden können. Es handelt sich aber nicht, wie der Name suggerieren könnte, um ein Passwort für den Lesezugriff.

Die Spezifikationen sehen auch den Einsatz eines Zufallszahlengenerators vor.[586] Dennoch gibt es keine vollwertige Kryptofunktionalität (z.B. keine kryptographischen Hashfunktionen). Die vom Tag generierten und an den Reader im Klartext (aber mit schwächerer Sendeleistung) übermittelten Zufallszahlen benutzt dieser für eine XOR-Kodierung seiner stärkeren Signale, die z.B. Passwörter für Kommandos enthalten. Damit wird eine Einschränkung der effektiven Abhörreichweite auf die geringere Antwortreichweite der Tags erreicht.

Zusammenfassend gesagt, es ist in diesen Tag-Klassen für den Massenmarkt keinerlei Schutz vor unerlaubtem Auslesen, Tracking und Profiling implementiert.

7.2.3.2.4.3 RFID-Tags mit stärkeren Kryptofunktionen

Eine zweite wichtige Kategorie bilden RFID-Tags, die zumindest symmetrische Kryptographie wie (3)DES oder AES einsetzen können (Symmetric-key Tags[587]). Diese Tags eignen sich im Allgemeinen auch zur Bereitstellung kryptographischer Hashfunktionen wie MD5 oder SHA-1. [588]

Die stärkste Anforderung wäre aus Sicherheitssicht der Einsatz von Public-Key Kryptographie, die allerdings auch die stärksten Leistungsanforderungen stellt. Die zugehörige Hardware wird sich vermutlich den Leistungsdaten von heutigen Sensornetz-Knoten annähern, wo es seit kurzem erste Implementierungen von asymmetrischer Kryptographie vor allem mittels Elliptischer Kurven (ECC) gibt.[589] Die Kosten werden aber wohl auf absehbare Zeit weitaus höher sein als bei EPC Class-1 Tags.

Für EPCglobal Class-2 Tags ist laut Class-1 Gen. 2 Spezifikation eine Form von authentifi-

---

[584] EPCglobal Radio-Frequency Identity Protocols – Class-1 Generation-2, 2004/2005.

[585] Die Spezifikationen für Class-1 sahen ebenfalls ein optionales Kill-Passwort vor (Länge 24 Bit).

[586] Ibid., S. 40.

[587] Juels, 2005, S. 7. Ohkubo et al., 2005, sprechen von „smart tags“. In der Klassifikation BSI, 2004, S. 38, entsprechen diese Tags einer Zwischenkategorie zwischen „Mittlerer Leistungsfähigkeit“ und „High-end“.

[588] Alle genannten Verfahren dienen als Beispiele; auf ihre möglichen und tatsächlichen Sicherheitsmängel soll an dieser Stelle nicht eingegangen werden.

[589] Gupta et al., Sizzle – a standards-based end-to-end security architecture for the embedded Internet, PerCom 2005, S. 247–256; Blaß / Zitterbart, Acceptable Public-Key Encryption in Sensor Networks, 2005. Zu ECC allgemein: Hankerson, 2004.

zierter Zugriffskontrolle[590] vorgesehen, deren Umfang und Art der Implementierung noch nicht veröffentlicht ist. Generell kann man für die Tags der höheren Klassen parallel zu den übrigen Leistungsdaten bessere Schutzfunktionen erwarten.

Unabhängig von den vorgegebenen Standards existieren bereits Prototypen von RFID-Tags mit einer Implementierung von AES-128.[591]

7.2.3.2.5 Zugriffskontrolle bei RFID

Bereits das Auslesen einer einfachen Identifikationsnummer[592] (z.B. eines EPC) auf einem Tag wirft genauso wie ein über Funk lesbarer Reisepass das klassische Problem der Zugriffskontrolle (Access Control) auf. Wir beschränken uns hier exemplarisch auf RFID, einen Überblick für allgemeines UC bieten z.B. Yamada / Kamioka, 2005.

Als ausführliches Beispiel für Zugriffskontrolle bei Tags mit starken Kryptofunktionen wird zunächst die Konzeption des EU-Reisepasses behandelt, wo das RFID-Interface mit einem Chip von der Leistungsfähigkeit einer Smart Card kombiniert wird. Paradigmatisch nicht nur für UC ist, dass selbst unter diesen guten Leistungsvoraussetzungen und einer sorgfältigen Planung des Systems Sicherheitslücken entstanden sind.

Ähnliche Kombinationen von RFID mit klassischen Smart Cards erlangen bei ID- und Kundenkarten und Tickets zunehmend an Bedeutung,[593] werden sich aber vermutlich selbst mittelfristig aufgrund der Stückkosten und der Chipgröße weniger für den großflächigen Einsatz in Logistik und Handel eignen als EPC-Tags. Diesen einfacheren Tags für den Massenmarkt mit ihrer viel geringeren Sicherheitsfunktionalität widmet sich danach der Rest des Kapitels.

7.2.3.2.5.1 Beispiel: RFID-Einsatz im EU-Reisepass

Auf Grundlage der Verordnung des EU-Rates vom 13. Dezember 2004[594] sowie des Beschlusses der EU-Kommission vom 28. Februar 2005[595] wurden RFID-Chips als Trägermedium für die künftig in EU-Reisepässen enthaltenen biometrischen Daten gewählt. Die technische Realisierung, die auch im seit 2005 in der Bundesrepublik Deutschland eingeführten neuen Reisepass zum Einsatz kommt, folgt dabei den Empfehlungen der International Civil

---

[590] EPCglobal: Class-1 Generation-2, 2004/2005, S. 3.

[591] Feldhofer / Dominikus / Wolkerstorfer, 2004.

[592] Wird diese ID bereits zur Tag-Separierung (Antikollisionsverfahren) benutzt, hilft eine Zugriffskontrolle auf der Schicht des ID-Protokolls nicht mehr, s. Kap. 7.2.3.2.6.1.

[593] Salzmann, iX 4, 2006, S. 112-114.

[594] Verordnung (EG) Nr. 2252 / 2004 des Rates vom 13. Dezember 2004 über Normen für die Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/oj/2004/l_385/l_38520041229de00010006.pdf (06.03.2006).

[595] Entscheidung der Kommission vom 28. Februar 2005 über die technischen Spezifikationen zu Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, K (2005) 409, http://europa.eu.int/comm/justice_home/doc_centre/freetravel/documents/doc/c_2005_409_de.pdf (06.03.2006).

Aviation Organisation (ICAO[596]) für maschinenlesbare Reisedokumente (Machine-Readable Travel Documents, MRTDs).

Das entscheidende ICAO-Dokument Nr. 9303[597] ist in drei Teile für Pässe, Visa und offizielle Reisedokumente untergliedert. Der erste Teil für Pässe legt fest, dass der RFID-Chip verpflichtend Name, Nationalität, Geburtsdatum, Geschlecht und ein Foto des Passinhabers sowie Nummer, Ausstellungsdatum sowie das Ablaufdatum enthält. Eine Verschlüsselung der gespeicherten personenbezogenen Daten sowie der Übertragungsvorgänge ist nicht vorgeschrieben, jedoch optional ebenso möglich wie die Speicherung zusätzlicher personenbezogener Daten, z.B. von Fingerabdrücken oder Iris-Scans. Eine digitale Signatur der ausstellenden Instanz über die enthaltenen Daten wird erstellt und ebenfalls auf dem Chip gespeichert (zumindest innerhalb der EU-Spezifikationen).

Da es möglich ist, die Kommunikation zwischen RFID-Chip und Lesegerät über mehrere Meter Entfernung abzuhören,[598] wurde mit *Basic Access Control*[599] ein Mechanismus in die Reisepass-Spezifikation aufgenommen, der einen Zugriffsschutz implementiert. Dabei wird die optisch maschinenlesbare Zone des Passes (Machine-Readable Zone, MRZ), die einige der genannten Passdaten enthält, verwendet, um einen initialen Schlüssel für die Kommunikation zwischen Lesegerät und RFID zu bilden. Über die so entstandene verschlüsselte Verbindung authentisieren sich beide gegenseitig und handeln einen Sitzungsschlüssel für die weitere Kommunikation aus.[600]

Solange der initiale Schlüssel nicht an den RFID-Chip gesendet wird, antwortet dieser nicht auf Kommunikationsversuche. So sollen ein unbemerktes automatisiertes Verfolgen des Passinhabers (Tracking) oder unbefugte Ausleseversuche verhindert werden. Obgleich Basic Access Control in den Empfehlungen der ICAO nur optional vorgesehen ist, wird dies in den Reisepässen der EU jedoch durchgängig implementiert.

Bereits im Sommer 2005 wurde gezeigt, dass die Entschlüsselung einer abgehörten Kommunikation zwischen Lesegerät und RFID-Chip eines niederländischen Passes mit einem PC innerhalb von ca. zwei Stunden durchführbar ist,[601] da aufgrund von Regelmäßigkeiten der Passnummern und Relationen zwischen diesen und den Daten von Ausstellung und Gültigkeit der zu testende Schlüsselraum deutlich geringer als angenommen ist. Von dieser Beeinträchtigung der Sicherheit sind auch die deutschen und österreichischen Pässe betrof-

[596] ICAO Homepage, http://www.icao.int/, insb. http://www.icao.int/mrtd/Home/Index.cfm zu maschinenlesbaren Reisedokumenten (06.03.2006).

[597] ICAO, MRTD Document 9303, vergl. http://www.icao.int/mrtd/publications/doc.cfm (06.03.2006).

[598] Finke / Kelter, 2004.

[599] In früheren Publikationen auch Basic Authentication genannt.

[600] Kügler, Dennis: Risiko Reisepass? Schutz der biometrischen Daten im RF-Chip, c't 5/2005, http://www.heise.de/kiosk/archiv/ct/05/05/084/ (06.03.2006).

[601] Robroch, Harko: Privacy Issues with new digital passports, 2005, http://www.riscure.com/news/passport.html (06.03.2006).

fen.[602]

Wer im Besitz des Passes ist, besitzt bei Basic Access Control alle benötigten Geheimnisse (die in der MRZ enthaltenen Daten), um mit dem Chip zu kommunizieren. Da sich die MRZ der Pässe nicht ändert, wird für die Kommunikation stets der gleiche initiale Schlüssel verwendet. Daher kann jeder, der einmal optischen Zugriff auf die MRZ hatte, diese speichern und für eine zukünftige automatisierte Erkennung des Passes (und darüber des Trägers) verwenden. Zudem sind in diversen Ländern Hotels verpflichtet, sich die Pässe ihrer Gäste vorübergehend aushändigen zu lassen. Aus diesen Gründen ist die MRZ kein geeignetes Geheimnis für den Schutz einer Übermittlung personenbezogener Daten.

Bei Verwendung spezifikationskonformer Lesegeräte ist die Kommunikation zu den in den Pässen enthaltenen RFID-Chips nur über Distanzen im Zentimeterbereich möglich. Allerdings kann durch die Verwendung von nicht-standardkonformen Lesegeräten und erhöhtem technischen Aufwand die Reichweite für das aktive Auslesen erhöht werden.[603]

Aus der mangelnden Eignung der MRZ als Geheimnis sowie der gegenüber dem Standard vergrößerbaren Auslesereichweite lassen sich diverse Szenarien ableiten, die neben der informationellen Selbstbestimmung auch Leib und Leben der Passinhaber gefährden könnten.[604]

In einer zweiten Ausbaustufe sollen die EU-Reisepässe um weitere biometrische Daten (zunächst Fingerabdruck) sowie mit *Extended Access Control* um einen erweiterten Zugriffsschutz ergänzt werden.[605] Dabei wird ein zusätzlicher Public Key-Authentifizierungsmechanismus eingeführt, für den das Lesegerät mit einem eigenen Schlüsselpaar und einem vom RF-Chip verifizierbaren Zertifikat ausgestattet werden soll. Durch das Zertifikat werden die Berechtigungen des Lesegerätes festgelegt. Dabei bestimmt immer die Passaustellende Instanz, auf welche Daten ein (z.B. ausländisches) Lesegerät zugreifen darf. Zu Extended Access Control sind bisher noch keine Spezifikationen öffentlich verfügbar, so dass eine unabhängige Evaluierung, die vor einer Einführung noch erfolgen sollte, bisher nicht vorliegt.

Die Einführung der RFID-Chips in den Ausweisen erreicht zwar durch die enthaltene digitale Signatur der ausstellenden Behörde über die personenbezogenen Daten eine erhöhte Fälschungssicherheit des Dokuments, führt aber zu einer deutlichen Gefährdung mindestens der informationellen Selbstbestimmung der Passinhaber.

Das Verfahren Basic Access Control (und ggf. das darauf aufsetzende Extended Access Control) sollte daher so überarbeitet werden, dass die Sicherheit der Kommunikation nicht mehr von der MRZ abhängt, sondern z.B. von der Eingabe eines Geheimnisses durch den Pass-Inhaber, das nur diesem bekannt ist. Dadurch würde der Transfer der Daten vom Be-

---

[602] Roth, Wolf-Dieter, Niederlande: Biometrie-Pass erfolgreich gehackt, 2006, http://www.heise.de/tp/r4/artikel/21/21907/1.html (06.03.2006).

[603] Kügler, Risiko Reisepass?, op. cit.

[604] Für ein Extrembeispiel vergl. das Konzept einer personenspezifischen Bombe in Pfitzmann, 2005.

[605] Kügler, BSI-Kongress 2005.

troffenen aktiv autorisiert. Ein ähnliches Verfahren hat sich z.B. mit der Eingabe einer PIN bei den Inhabern von EC-Karten als praktikabel und alltagstauglich erwiesen. Da EC-Karten vermutlich deutlich häufiger zum Einsatz kommen als Reisepässe, wobei sie ebenso ständig mitgeführt werden und zudem seit mehreren Jahren in Umlauf sind, könnte dieses Verfahren ggf. mit einigen Modifikationen auch im Fall der Reisepässe zur Anwendung kommen.

7.2.3.2.5.2 Zerstören oder Entfernen der Tags

Die physische Zerstörung oder das Entfernen der Tags vor oder beim Verkauf als extreme Form der Zugriffskontrolle (niemand darf zugreifen) würde einerseits die Vorteile des Einsatzes von RFID in der Logistik erhalten, andererseits die informationelle Selbstbestimmung des Individuums im Alltag bewahren.

Die Nutzung der Tags für weitere Dienste wie etwa in Smart Homes (z.B. mit „intelligenter" Waschmaschine oder Kühlschrank) wäre damit aber ausgeschlossen.

Problematisch ist ebenfalls der genaue Zeitpunkt einer Zerstörung: Erfolgt sie erst beim oder nach dem Bezahlvorgang, so bleiben Kunden im Verkaufsareal ortbar, ihre Bewegungen verfolgbar und die Kombination der gewählten Produkte erfassbar, auch wenn sie diese ggf. wieder ins Regal zurückstellen. Erfolgt die Zerstörung vorher, lassen sich logistische Vorteile für den Verkaufspunkt selbst (etwa Verhindern der „Out-of-shelf"-Situation, Optimierung von Werbung und Verkaufsflächen) nicht mehr umsetzen.

Bleibt hingegen die Zerstörung der Tags als alleinige Schutzmaßnahme den Nutzern überlassen[606], so besteht die Gefahr, dass sie aus Bequemlichkeit mit der Zeit unterbleibt.

Schließlich ergibt sich die Frage, wie gründlich eine physische Zerstörung abläuft. Sollte ein EPC danach mit geeigneten Werkzeugen immer noch auslesbar sein, so bleibt zumindest das Problem der langfristigen Objektverantwortung bestehen.

7.2.3.2.5.3 „Clipped Tags" mit visueller Bestätigung der Deaktivierung

Wie kann ein Nutzer sicher sein, dass ein vorgeblich zerstörter RFID-Tag wirklich funktionsunfähig ist? Eine systematische Lösung stellen Ansätze dar, die Zerstörung des Kontakts vom Chip zur Antenne mit einer sichtbaren Bestätigung zu verbinden.[607] Die Antenne kann zum Beispiel eine Art Sollbruchstelle mit einem kleinen Griff besitzen, dessen Betätigung den Kontakt zum eigentlichen Chip abschneidet. Andere Möglichkeiten sind durch Rubbeln entfernbare Antennen oder abziehbare Folien.[608]

Vorteil dieser Methode ist, dass Nutzer den Zeitpunkt der Zerstörung selbst wählen können und mehr Kontrolle über den Vorgang besitzen. Tracking und Auslesen von Besitz wird bei dieser Form der Deaktivierung sehr erschwert. So soll die Auslesereichweite ohne Antenne

[606] Z.B. mithilfe eines tragbaren „RFID-Zappers" als Extremform einer permanenten Zugriffsverweigerung: https://events.ccc.de/congress/2005/wiki/RFID-Zapper (31.01.2006).

[607] Karjoth / Moskowitz, 2005; Karjoth, 2005.

[608] Heise Newsticker, 14.03.2006: http://www.heise.de/newsticker/meldung/70778 (14.03.2006).

noch 5 cm betragen.[609]

Nachteilig ist, dass es sich um eine Opt-out-Lösung handelt, d.h. per Default sind die Tags aktiviert, und Aufwand und Sorgfalt der Deaktivierung liegen beim Kunden, was bei einem größeren Einkauf Mühe machen wird. Ferner ist aus Sicht des Datenschutzes negativ, dass der eigentliche Chip, der den EPC speichert, nicht zerstört wird und mit höherem technischen Aufwand auslesbar bleibt. Explizit wird die Möglichkeit genannt, eine neue Antenne anzubringen.[610] Somit bleibt die Gefahr der langfristigen Objektverantwortlichkeit bei EPCs, die irgendwann (wie etwa beim Kauf mit Kredit- oder EC-Karte) mit persönlichen Daten verknüpfbar wurden, bestehen.

7.2.3.2.5.4 „Kill"-Kommando

Wie oben bereits angeführt, sieht der EPCglobal Class-1 (Generation 2) Standard[611] ein sogenanntes „Kill-Passwort" von 32 Bit Länge vor. Dieses Passwort ermöglicht es einem RFID-Reader, einen Tag, der sich an diese Spezifikationen hält, permanent zu deaktivieren. Das Kill-Kommando benötigt als Teil des Standards keine Modifikation an der Hardware dieser einfachen EPC-Tags.

Unklar ist, ob der gespeicherte EPC auf dem Chip erhalten bleibt. Es gibt keine sichtbare Bestätigung, ob der Vorgang erfolgreich war. Fraglich ist auch die Skalierbarkeit: Die notwendige Absicherung des Vorgangs mit einem Passwort wirft ein Passwort-Management-Problem auf. Falls die Deaktivierung im Laden geschehen soll, ist sie so gestaltet, dass sie schnell und ohne merklichen Aufwand geschehen kann? Wenn hingegen der Endkunde selbst seine RFID-Tags deaktivieren möchte, wie und wo kann er die nötige Vielzahl an Passwörtern speichern und organisieren? Bei Schwächen der Passwortfunktionalität besteht zudem die Gefahr eines DoS-Angriffes gegen bewusst nicht deaktivierte Tags.

Die permanente Deaktivierung schließt den Tag auch von nachgelagerten Dienstleistungen aus. Sollten deren objektive Vorteile oder auch nur ein entsprechendes Marketing dazu führen, dass Tags immer häufiger nicht deaktiviert werden, so ist keine weitere Schutzfunktion vorhanden.

7.2.3.2.5.5 Stören des Leseversuchs

Anstatt die Tags zu deaktivieren, könnte man versuchen, jedes Mal, wenn ein Reader einen Auslesevorgang starten möchte, Störmaßnahmen zu ergreifen. Eine einfache Abschirmung der Tags durch metallbeschichtete Behältnisse oder Flüssigkeit ist ohne unzumutbaren Aufwand nur für einzelne Tags möglich, sofern und solange diese nicht fest in Kleidung oder andere Gegenstände integriert sind. Wir geben einen kurzen Überblick über andere Vorschläge.

---

[609] Heise Newsticker, 10.03.2006: http://www.heise.de/newsticker/meldung/70646/ (14.03.2006).

[610] Heise Newsticker, Meldung 70778, op. cit.

[611] EPCglobal Radio-Frequency Identity Protocols – Class-1 Generation-2, 2004/2005.

Störsender

Der Betrieb von Störsendern auf den für RFID üblichen Funkfrequenzen[612] würde nicht nur die eigenen Tags schützen, sondern in der gesamten Sendereichweite die Funktion von anderen RFID-Systemen stark behindern. Ihr Einsatz wäre mit hoher Wahrscheinlichkeit nicht zulässig.

Blocker Tags

Eleganter als Störsender gehen so genannte „Blocker Tags“[613] vor (im Folgenden BT genannt). Sie machen sich das MAC[614]–Protokoll der Kommunikation zwischen RFID-Tag und Reader zu Nutze, das als Antikollisionsverfahren entweder „Treewalking“ oder – ein BT ist dafür bisher nur theoretisch – eine Form von Aloha[615] vorsieht, um einem Reader das gleichzeitige Auslesen mehrerer Tags zu ermöglichen.

Beim Treewalking werden die Identifikatoren der beteiligten Tags, üblicherweise der EPC[616], in einen binären Suchbaum eingebettet, in dem der Reader eine Tiefensuche[617] ausführt: Bit für Bit werden die sendebereiten Tags separiert, bis nur noch ein Identifikator feststeht, dessen Tag jetzt senden darf.

Ein BT ist nun ein zusätzlicher Tag im Besitz desjenigen, dessen Tags vom Reader ausgelesen werden soll. Der BT meldet sich in jedem Schritt des Separierungsprotokolls, also nicht nur regulär genau dann, wenn das Suchpräfix seinem Identifikator entspricht. Damit täuscht er dem Lesegerät eine maximale Population von Tags vor, denn jeder Identifikator scheint anwesend zu sein, so dass es eine sehr lange Zeit mit dem Separieren der virtuellen Tags benötigt – in dieser Zeit kann es keine anderen Leseoperationen ausführen. Ein BT für das Aloha-Protokoll könnte immer dann antworten, wenn es möglich ist – und nicht erst nach zufälligen Wartezeiten, wie eigentlich vorgesehen. Energie ist hierbei kein prinzipielles Hindernis, da ein BT auch als aktives Gerät mit eigener Energieversorgung denkbar ist.

Eine Ergänzung des BT ergibt sich durch die Verwendung einer „Privacy-Zone“[618] bei den binären Tag-Identifikatoren: So könnten geheim zu haltende IDs mit einer führenden 1 versehen werden, und der BT nur beim illegitimen Versuch, diesen privaten Teilbaum zu separieren, in Aktion treten.

---

[612] Mögliche Frequenzen für EPC-Tags: 13.56 MHz (HF, ISM-Band) oder 860 MHz – 930 MHz (UHF) bei Class-1 Gen-1 Tags, 860 MHz – 960 MHz (UHF) Class-1 Gen-2.

[613] Juels et al., 2003; Juels, 2005.

[614] Medium Access Control, d.h. Regelung des Zugriffs auf das Funkmedium.

[615] „Slotted random anticollision“ bei Class-1 Gen-2 Tags: Tags warten eine zufällige Zeit, bevor sie antworten. Siehe z.B. Finkenzeller, 2002, S. 210ff. Der bisher publizierte BT von RSA funktioniert nur mit Treewalking.

[616] Die Verwendung des EPCs in dieser Funktion wirft zusätzliche Datenschutzprobleme auf, s.u. Kap. 7.2.3.2.6.1.

[617] Depth First Search (DFS): Die Suche folgt zuerst einem Pfad in die Tiefe des Suchbaums.

[618] Juels et al., op. cit., 2003.

Da ein BT die eigenen Tags vor jedem Reader abschirmt, findet keine Selektion etwa nach erwünschten oder unerwünschten Lesegeräten statt. Nutzer haben außerdem kaum eine Möglichkeit zu verifizieren, ob ein Auslesevorgang wirklich durch einen BT blockiert wurde – eine Restunsicherheit bleibt.

Die Einführung einer Privacy-Zone z.B. in einem Bit des EPC-Headers müsste für offene, globale Systeme – wie RFID auf Einzelprodukten – auch zu einem globalen Standard werden. Nur so könnte man sicher sein, ausschließlich irreguläre Ausleseversuche zu verhindern.

Schließlich verhindert ein BT nicht nur das Auslesen der eigenen Tags, sondern aller Tags in seiner Reichweite. Somit ist auch mit starken Beeinträchtigungen Dritter zu rechnen. Insgesamt erscheinen BT vielleicht in Spezialfällen anwendbar, sie stellen aber keine solide Schutzlösung dar.

7.2.3.2.5.6 Authentifizierung des Readers beim Tag

Die zentralen Probleme des Auslesens von Besitz und des Trackings von Personen machen grundlegende Maßnahmen erforderlich, die bisher nicht ausreichend in den RFID-Tags für den Massenmarkt umgesetzt sind. Eine grundlegende Anforderung ist die Authentifizierung des RFID-Readers beim Tag, bevor überhaupt Daten wie z.B. ein EPC ausgelesen werden können. Aufgrund der schwachen Leistungsdaten von RFID-Tags jedoch gestaltet sich eine sichere Umsetzung dieser Anforderung äußerst schwierig.

Passwortschutz

Eine klassische Authentifizierungsmethode ist ein Passwortschutz, bei dem sich Tag und Reader ein gemeinsames Geheimnis (das Passwort) teilen. Der Reader muss mittels eines vereinbarten Protokolls nachweisen, dass er im Besitz dieses Geheimnisses ist.

Das Passwort selbst sollte keinesfalls im Klartext über eine Funkschnittstelle übertragen werden. Eine übliche Lösung dafür sind sogenannte Challenge-Response-Verfahren, wie sie z.B. auch in der ISO-Norm 9798[619] aufgeführt werden.[620] Dabei wird das Passwort nicht direkt übertragen, sondern stattdessen ein mit dem Passwort verschlüsselter[621] Wert, der beiden Kommunikationspartnern bekannt ist und auch von Dritten in Erfahrung gebracht werden darf. Der Empfänger verschlüsselt den Wert genau wie der Sender mit dem gemeinsamen Passwort; stimmt das eigene mit dem empfangenen Ergebnis überein, so geht er davon aus, dass der Sender das Passwort kennt und somit autorisiert ist.

Wichtig ist es dabei sicherzustellen, dass die empfangene Nachricht keine Wiederholung (Replay) einer echten, älteren Authentifizierung ist. Darum sollte der Tag fähig sein, den zu verschlüsselnden Wert möglichst zufällig und stets neu zu generieren, was einen Pseudozu-

[619] ISO 9798, 1997 / 1999.

[620] Anwendung für RFID z.B. bei Finkenzeller, 2002, S. 225ff.; BSI, 2004, S. 49.

[621] Symmetrische Verschlüsselung oder HMAC, d.h. Hashfunktion mit Schlüssel als zusätzlichem Input, siehe Krawczyk, RFC 2104, 1997.

fallsgenerator (PRNG) auf dem Tag notwendig macht.

Die bisher in den Standards von EPCglobal vorgesehene Passwortfunktionalität schützt nicht den Lesezugriff auf die gespeicherte Identifikationsnummer (EPC) eines Tags. Um die Privatsphäre des Individuums zu wahren, müssen die bisherigen EPCglobal Tag-Reader-Spezifikationen und Protokolle entsprechend angepasst werden.

Wieder verwendbare Passwörter gelten allerdings in der Informationssicherheit – trotz ihrer weiten Verbreitung – als sehr schwache Schutzmaßnahme, die z.B. durch Mehrfaktor-Authentifizierung[622] oder Einmalpasswörter abgelöst werden sollte. Beides stellt eine gewaltige Anforderung an die begrenzten Tag-Ressourcen dar. Passwortschutz skaliert im Allgemeinen nur gut in eng umgrenzten, geschlossenen Systemen.

Ferner besteht die Gefahr von Brute-Force-Angriffen: Ist die Passwortlänge zu kurz und wird die Anzahl der möglichen Fehlversuche pro Zeiteinheit nicht begrenzt, so besteht die Gefahr, dass Angreifer einfach automatisiert alle möglichen Passwörter durchprobieren.[623] Werden z.B. in einem Geschäft alle Waren-Tags zunächst mit dem gleichen Passwort versehen, resultiert aus einem außerhalb des Geschäftes erfolgreich durchgeführtem Brute-Force-Angriff ein Gefährdungspotential (z.B. Denial-of-Service-Angriff) für alle Tags innerhalb des Geschäfts.

Beispiel: Das „Passwort-Modell“

Ein konkreter Gestaltungsvorschlag eines Passwortschutzes für RFID-Tags auf Einzelprodukten ist das „Passwort-Modell“.[624] Hier wird auf den Tags anstelle der „Kill“-Funktion eine (De-)Aktivierungsfunktion implementiert, die insbesondere den Lesezugriff auf den im Tag gespeicherten EPC regelt. Ist der Tag im Sinne dieser Lösung aktiviert, verhält er sich wie ein üblicher ungeschützter EPC-Tag, nimmt an Separierungsprotokollen teil und gibt seinen EPC jedem Lesegerät preis.

Mittels eines speziellen Deaktivierungspassworts wird der Tag in einen sichereren Zustand versetzt („deaktiviert“): Der Tag verlangt nun nach dem RFID-Separierungsvorgang ein „RFID-Passwort“, das der Kunde an der Supermarktkasse, z.B. mithilfe einer Datenschutzkarte, setzen kann.

Für die Nutzung von Diensten nach dem Kauf, die mittels RFID im Sinne des Kunden erbracht werden sollen, kann der Besitzer nun dem jeweiligen Dienstbetreiber (wie z.B. seinem eigenen „intelligenten“ Kühlschrank zur Wareninventarisierung) das RFID-Passwort zur Verfügung stellen, um die Tags auch im deaktivierten Zustand nutzen zu können.

---

[622] Grundprinzip: „Something you *know* and something you *have*“, z.B. PIN und Bankkarte.

[623] Ein Beispiel für einen praktisch durchgeführten Angriff auf den 40 Bit-Schlüssel des „SpeedPass“-RFID-Systems vieler amerikanischer Tankstellen bieten Bono et al., 2005.

[624] Berthold / Günther / Spiekermann, Wirtschaftsinformatik 6 (47), 2005, S. 422–430.

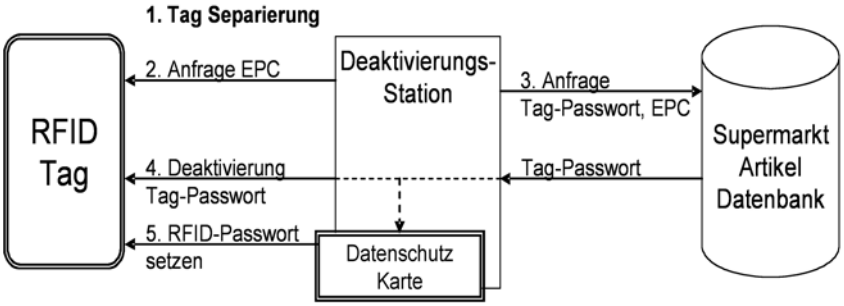


Abbildung 35: Prozessablauf beim „Passwort-Modell“ (Berthold et al., 2005)

In einer einfachen Variante wird das Passwort im Klartext übertragen, um weniger Änderungen an den Tags vornehmen zu müssen. Diese Grundversion mit Passwortübertragung im Klartext über eine Funkschnittstelle erscheint aus Sicherheitssicht höchst fragwürdig, auch wenn sie nach Meinung der Autoren zumindest einen gewissen Schutz vor heimlicher Massenüberwachung bietet. Eine erweiterte Version benutzt daher ein Challenge-Response-Verfahren, wie es oben beschrieben wurde.

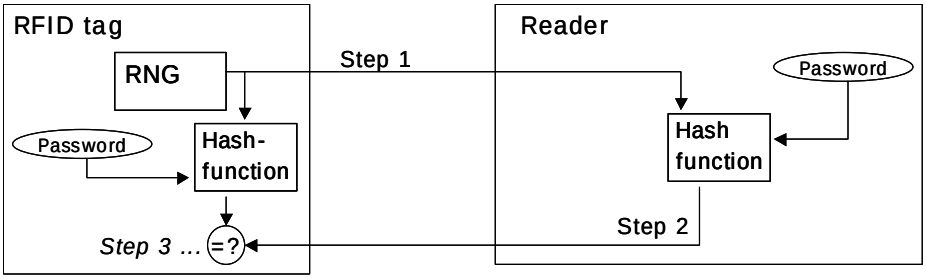


Abbildung 36: Challenge-Response beim erweiterten „Passwort-Modell“ (Berthold et al., 2005)

Sichere Skalierbarkeit, d.h. insbesondere das Schlüsselmanagement, stellt sich hierbei als ein fundamentales Problem dar, wie die Autoren anführen:[625] „Hätte jeder RFID-Tag [eines bestimmten Nutzers] ein anderes Passwort, wäre ... eine Tag-Kennung erforderlich, die auch im deaktivierten Zustand ausgesendet wird, um dem Lesegerät die effiziente Ermittlung des richtigen Passwortes zu ermöglichen“, was Tracking anhand der Kennung ermöglichen würde. Daher ist in diesem Modell das RFID-Passwort eines Nutzers für alle seine Gegenstände am Körper und zu Hause dasselbe.

Ein über einen längeren Zeitraum konstantes gemeinsames Passwort für viele Tags, die zu verschiedensten Gelegenheiten an diversen Orten in Verwendung sind, erscheint jedoch riskant, denn nur eine einmalige Kompromittierung ist notwendig, um Zugang zum gesamten Inventar einer Person zu erhalten. Besser erscheinen daher Verfahren der Authentifizierung mit abgeleiteten Schlüsseln[626], wo aus einem gemeinsamen Masterschlüssel die Schlüssel der einzelnen Tags generiert werden.

[625] Berthold / Günther / Spiekermann, op. cit.

[626] Finkenzeller, op. cit., S. 227f.

Wichtig ist außerdem, wie das Passwort bei der Übertragung zwischen Karte und Reader (oder Backend zur Generierung einer Antwort) gesichert wird.

Selbst wenn Dritte keinen Zugang erhalten, kann der Betreiber des Readers das Passwort unbemerkt dauerhaft speichern. Bei diesem Verfahren wäre also eine starke rechtliche Flankierung verbunden mit häufigen Audits notwendig.

Wie oft und wie leicht kann ein Nutzer das Passwort auf allen seinen Gegenständen ändern? Erfahrungen aus der klassischen IT-Sicherheit zeigen, dass solche Änderungsvorgänge selbst bei gut informierten Nutzern meist nur mit gewissem Zwang durchzusetzen sind; man wird daher erwarten müssen, dass ein überwiegender Teil der Nutzer sein RFID-Passwort selten oder gar niemals wechseln würde.

7.2.3.2.5.7 Authentifizierung des Tags beim Reader

Für viele industrielle Anwendungen von RFID, wie etwa die Gewährleistung von Fälschungssicherheit von Waren oder Ersatzteilen, steht das umgekehrte Authentifizierungsproblem im Mittelpunkt: Ein Tag soll sich beim Reader authentifizieren und damit z.B. die Echtheit des mit ihm verbundenen Objekts nachweisen.

Nach Ansicht des BSI bietet „eine weltweit eindeutige Regelung zur Vergabe der ID-Nummern (Seriennummer) von Tags, ... z.B. EPC ... einen gewissen Schutz vor gefälschten Tags“[627], wobei allerdings dieser Schutz durch freie Auslesbarkeit von Seriennummern und beschreibbare Tags schnell seine Grenzen finden könnte.

Zur Durchführung einer besseren wechselseitigen Authentifizierung des Tags beim Reader kann auch das bereits beschriebene Challenge-Response-Verfahren eingesetzt werden.

Hierzu kann auch eine Nachfrage nach für mit starken Kryptofunktionen ausgestatteten Tags entstehen, die wiederum auch für die oben dargestellte Authentifikation des Readers beim Tag genutzt werden könnte, indem das Verfahren doppelt ausgeführt wird, so dass beide Kommunikationspartner einander den Besitz des gemeinsamen Geheimnisses beweisen.[628]

Natürlich kann es durchaus im Interesse der Selbstbestimmung des Individuums sein, dass sich RFID-Tags gegenüber Dienstanbietern authentifizieren müssen, z.B. die Tags in Zugangskarten gegenüber Türen oder Computern oder Tags in Autoschlüsseln gegenüber dem Fahrzeug, um Identitäts- oder auch realen Diebstahl zu verhindern. Wichtig sind hier ein datenschutzfreundliches Protokolldesign und die Frage, inwieweit die Anonymität der Nutzer dadurch beeinträchtigt wird.

7.2.3.2.6 Sicherung der Kommunikation zwischen Tag und Reader

Nicht nur die Authentifizierung von Tag und Reader ist wichtig für die Informationssicherheit der beteiligten Systeme, sondern auch, inwieweit der gesamte Kommunikationsvorgang und Inhalt vor Dritten gesichert ist. Da Funkkommunikation leicht und unauffällig abgehört werden kann, benötigt wirksame Zugriffskontrolle (Kap. 7.2.3.2.5) insbesondere die Integrität

[627] BSI, 2004, S. 47.

[628] Finkenzeller, op. cit., S. 225-227.

und Authentizität des Datenkanals und Vertraulichkeit bei der Übertragung von Nutzdaten. Der folgende Abschnitt zeigt aber zunächst auf, wie schwierig es ist, die Kommunikation gegen Tracking, d.h. Angriffe auf die Vertraulichkeit des Aufenthaltsortes (Location Privacy) zu sichern.

7.2.3.2.6.1 Tracking: Ein „vielschichtiges“ Problem

Das Problem, unerwünschte Identifikation und Tracking von Menschen durch RFID zu vermeiden, ist nicht auf das eigentliche Identifikationsprotokoll (Beispiel: Der Tag nennt seinen EPC) beschränkt. Bevor entsprechende Bedenken im Zusammenhang mit dem Einsatz von RFID in Reisepässen laut wurden[629], wurde bereits in der Forschung[630] darauf hingewiesen, dass wie bei anderen Funktechniken wie WLAN und Bluetooth[631] auch bei RFID Identifizierbarkeit und Tracking auf verschiedenen Schichten eines Kommunikations-Modells[632] erfolgen kann, also nicht nur auf der Anwendungsschicht, die dem protokollkonformen Auslesen des EPC entspricht.

So verwenden die üblichen Antikollisionsprotokolle bei RFID, die zur Regelung des Medienzugriffs Bestandteil einer Sicherungsschicht unterhalb der Anwendungsschicht bilden, eindeutige Identifikatoren für die Tags.[633] Selbst wenn man hierfür nicht den EPC verwendet, sondern einen anderen festen Identifikator, lässt sich damit ein Tag einfach identifizieren und verfolgen. Eine Lösung hierfür ist es, die Antikollisonsprotokolle besser gegen Mithörer zu schützen, wie z.B. mittels des „Silent-Tree-Walking“-Protokolls[634].

Sicherer erscheint die Idee, einen anderen Identifikator als den des eigentlichen Identifikationsprotokolls zu benutzen und ihn nach jedem Einsatz zufällig neu zu generieren.[635] Die Güte der generierten Pseudozufallszahlen muss entsprechend hoch sein, z.B. sollten keine Regelmäßigkeiten in der Zahlenfolge erkennbar sein.

Höchst bedeutsam und hinsichtlich ihrer Tragweite öffentlich noch weitgehend unerforscht ist auch die Möglichkeit, Geräte im UC – und RFID-Tags im speziellen – anhand ihres Funk-„Fingerabdrucks“ eindeutig zu identifizieren, was einem Tracking auf der Bitübertragungs-

---

[629] Schneier, Cryptogram, 15. November 2005: http://www.schneier.com/crypto-gram-0511.html#1 (31.01.2006).

[630] Weis, 2003, und ausführlich Avoine / Oechslin, 2005.

[631] Hier sind besonders vom durchschnittlichen Nutzer schwer zu ändernde MAC- und Geräteadressen der Sicherungsschicht relevant, beim Einsatz von Mobile-IP natürlich besonders auch die IP-Adresse.

[632] Z.B. ISO/OSI-Schichtenmodell.

[633] Zumindest bei deterministischen Protokollen wie dem „Treewalking“ sind Identifikatoren unabdingbar. Laut Avoine / Oechslin, 2005, S. 10, werden Identifikatoren bei ALOHA-Protokollen zur Effizienzsteigerung eingesetzt.

[634] Weis et al., 2004.

[635] Heise News-Ticker, 16.11.2005: Laut BSI sei eine Randomisierung des Separationsidentifikators zumindest im europäischen Reisepass vorgesehen. http://www.heise.de/newsticker/meldung/66273 (31.01.2006).

schicht entspricht.[636]

7.2.3.2.6.2 Verschlüsselte Kommunikation

Um Identifikation, Profiling und Tracking durch Dritte, die die Kommunikation zwischen Tag und Reader mithören, zu verhindern, sollte diese nicht nur authentifiziert, sondern auch verschlüsselt ablaufen, auch wenn „nur" ein EPC übertragen wird. Werden auf leistungsfähigeren Tags[637] mehr Daten als ein Identifikator gespeichert (Prinzip „Data on Tag"), so gilt diese Anforderung in noch stärkerem Maße, insbesondere, wenn personenbezogene oder anderweitig sensible Daten enthalten sind.

Um diese Anforderung zu erfüllen, müssen genügend starke Kryptofunktionen auf den Tags vorhanden sein, z.B. die Möglichkeit zur symmetrischen Verschlüsselung. Implementierungen von AES auf RFID-Tags[638] zeigen die Umsetzbarkeit und geben Hoffnung auf marktfähige Kosten solcher Tags in nicht allzu ferner Zukunft.

Doch auch hier stellt sich das Problem eines nutzerfreundlichen und sicheren Schlüsselmanagements, das besonders für allgemeine Tag-Reader-Interaktionen in offenen Systemen und in globalem Maßstab noch nicht zufriedenstellend gelöst ist. Hier besteht noch ein sehr hoher Forschungsbedarf.

7.2.3.2.7 Pseudonymisierung

Um den direkten Zugriff Unbefugter auf die im Tag gespeicherte Identifikationsnummer wie z.B. einen EPC zu verhindern, kann man statt ihrer Pseudonyme verwenden. Im Folgenden betrachten wir einige Verfahren, die diesen Ansatz wählen.[639]

7.2.3.2.7.1 Hash-Lock und randomisiertes Hash-Lock-Verfahren

Das Hash-Lock-Verfahren[640] geht vom Vorhandensein einer Hashfunktion auf den verwendeten Tags aus, die zwei Zustände, offen (unlocked) und verschlossen (locked), kennen. Zusätzlich zu der normalen ID wird auf den Tags der Hashwert h=hash(z) einer tagspezifischen, zufällig generierten aber danach festen Zahl z gespeichert, sowie der Ursprungswert z selbst. Eine Backend-Datenbank für alle im System verwendeten Tags speichert die Paare (z, ID) unter der Verwendung von h als Primärschlüssel.

Der Hashwert h dient als Pseudonym des Tags (in der Originalarbeit „metaID" genannt). Nach der Speicherung des Pseudonyms gehen die Tags in den geschlossenen Zustand über, bei Leseversuchen verraten sie nun nur ihr jeweiliges Pseudonym h, nicht aber die eigentliche ID. Autorisierte Reader oder eine zugehörige Middleware können die Backenddatenbank befragen, um die zu h gehörige ursprüngliche ID für weitere Anwendungen zu ermitteln.

---

[636] Avoine / Öchslin, RFID Traceability: A Multilayer Problem, 2005, S. 138.

[637] Z.B. EPC-Tags höherer Klassen, die mehr Daten speichern können.

[638] Feldhofer / Dominikus / Wolkerstorfer, 2004.

[639] Überblick auch in BSI, 2004; Berthold / Günther / Spiekermann, op. cit.

[640] Weis et al., 2004. Ebendort auch das randomisierte Hash-Lock-Verfahren.

Um einen Tag wieder in den offenen Zustand zu versetzen, liest der Reader das zu h gehörige Urbild z aus der Datenbank, übermittelt z als eine Art Passwort (aber im Klartext) zum Tag, der daraufhin in den offenen Zustand wechselt, wo er wieder allen Readern seine ID übermittelt.

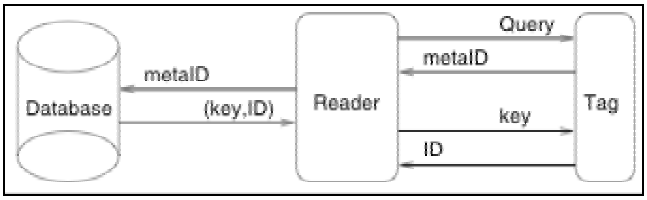


Abbildung 37: Hash-Lock-Verfahren, aus Weis et al., 2004

Das feste Pseudonym h allerdings kann anstelle der eigentlichen ID ebenfalls zum Tracking missbraucht werden. Darum geben die Autoren ein erweitertes Verfahren an, das randomisierte Hash-Lock-Verfahren. Hierbei muss ein Tag zusätzlich zur Implementierung einer Hashfunktion auch über einen Pseudozufallszahlen-Generator (PRNG) verfügen.

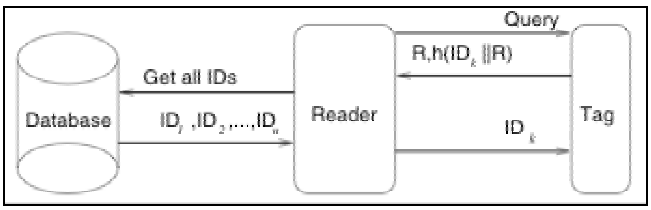


Abbildung 38: Randomisiertes Hash-Lock-Verfahren, aus Weis et al., 2004

In einer ersten randomisierten Variante antwortet ein Tag auf die Anfrage eines Readers mit einer Zufallszahl r und einem Hashwert h(ID||r). Um die Identität ID des Tags zu ermitteln, unternimmt der Reader oder ein Backend eine Suche mittels Brute-Force über alle bekannten IDs, d.h. er bildet für alle bekannten IDs h(ID||r). Wie die Autoren bemerken, eignet sich dieses Verfahren damit nur für eine kleine Gesamtzahl von Tags im System, z.B. alle Tags im Besitz einer bestimmten Person.

Die zweite randomisierte Variante benutzt einen symmetrischen Schlüssel k zwischen Tag und Reader als Parameter für eine Pseudozufallsfunktion; auch hier muss ein autorisierter Reader wiederum sämtliche im System vorhandenen IDs ausprobieren.[641]

Alle Verfahren skalieren nicht gut mit zunehmender Anzahl von Tags im System. Das einfache Verfahren verhindert Tracking nicht, und ist anfällig für Spoofing- bzw. Man-in-the-Middle-Angriffe, wo ein Angreifer das zu h gehörige Urbild z mitliest, nachdem er einem legitimen Reader das vom Tag bezogene h vortäuscht; der letzte Protokollschritt, in dem ein echter Tag sich mit seiner wahren ID authentifiziert, soll solche Angriffe zumindest erkennbar machen – ist der Angreifer allerdings schnell genug, könnte er die echte ID vom Tag empfangen und dem Reader protokollkonform präsentieren.

[641] Für einen Angreifer wäre der Suchraum größer, da er alle theoretisch möglichen IDs probieren müsste.

Das randomisierte Verfahren schützt zwar besser vor Tracking durch unautorisierte Reader, besitzt aber vergleichbare Schwächen wie die Grundversion. Wird einmal die ID im letzten Nachrichtenpaket von Reader zu Tag während eines autorisierten Unlock-Vorgangs mitgelesen, kann man sie jederzeit zum „Öffnen" des Tags benutzen (Replay-Angriff).[642]

7.2.3.2.7.2 „Private ID"-Verfahren

Beim „Private ID"-Verfahren[643] wird der global eindeutige Identifikator auf einem wieder beschreibbaren Tag einfach durch ein nur lokal eindeutiges Pseudonym ausgetauscht, das als Suchschlüssel in einer privaten Datenbank des Nutzers fungiert, um bei Bedarf die originale Identifikationsnummer zu finden.

Eine Abwandlung des Verfahrens für nicht wieder beschreibbare Tags kombiniert eine global eindeutige Seriennummer, z.B. eine Objektklasse (Class ID) und Seriennummer miteinander, die auch auf verschiedenen Tags gespeichert sein können. Nutzer können dann Teile der global eindeutigen Nummer anonymisieren, indem sie einen der zusammengehörigen Tags entfernen.

Der erste Ansatz, ein festes Pseudonym, hilft wie beim einfachen Hash-Lock-Verfahren zwar gegen das Auslesen des Besitzes, nicht aber gegen eine Lokalisierung und mögliche Identifikation des Besitzers, da das Pseudonym lokal eindeutig ist.

Ein änderbarer Identifikator auf dem Tag muss hingegen durch ein Zugriffskontrollsystem vor unbefugten Änderungen, z.B. zwecks Sabotage, geschützt werden.

Die Anforderung, eine Datenbank im Besitz des Nutzers zu haben, ist im Zuge fortschreitender Entwicklung des UC zwar nicht elegant, aber nicht zu stark, da vom zukünftigen Vorhandensein geeigneter Geräte beim Benutzer ausgegangen werden kann.

Beim zweiten Ansatz, der aufteilbaren Nummer, könnte durch das Beobachten von Tag-Clustern immer noch eindeutige Identifizierbarkeit und Verfolgbarkeit erreicht werden.

7.2.3.2.7.3 Tag-externe Verschlüsselung

Verschiedene Ansätze, stärkere Kryptographie mit Pseudonymisierung zu verbinden, verlegen die aufwendigen Berechnungsarbeiten vom Tag in das Backend der Reader-Infrastruktur.[644] Beim Auslesevorgang können autorisierte Reader einen erneuten externen Verschlüsselungsvorgang einleiten, der das Pseudonym auf den Tags ändert.

Zwischen den autorisierten Auslesevorgängen bleibt der Tag allerdings anhand seines aktuellen Pseudonyms ortbar. Skalierbarkeit und Sicherheit dieser Verfahren gerade in einem verteilten, großen System (wie dem Einsatz der Tags auf Einzelprodukten und verbundenen Diensten) sind höchst problematisch, da auch größere Teile der Reader-Infrastruktur vertrauenswürdig sein müssen – umso mehr, als häufiges Wiederverschlüsseln bei diesen Ver-

---

642 Ähnlich negative Beurteilung der Sicherheit in: BSI, 2004, S. 48 und S. 52.

643 Inoue / Yasuura 2003.

644 Z.B. Juels / Pappu, Squealing Euros, FC'03, 2003. Vergleichbar Ateniese / Camenisch / de Medeiros, CCS 05, 2005.

fahren notwendig gegen Tracking ist.

7.2.3.2.7.4 Hashbasierte Variation der Tag-ID

Ein anderes Verfahren[645], die Tag-ID mittels einer kryptographische Hashfunktion zu verschleiern, die auf den Tags implementiert sein muss, erfordert ebenfalls eine Datenbank im Besitz des Nutzers.

Die Grundidee ist, dass sich Tag und Datenbank anhand von Sessionnummern synchronisieren, wobei der Tag nach jedem autorisierten Lesevorgang sein Pseudonym so ändert, dass das Backend diese Änderung parallel nachvollziehen kann.

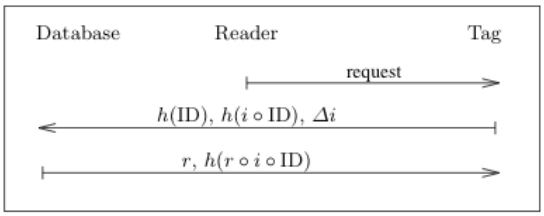


Abbildung 39: Hashbasierte ID-Variation (aus: Avoine / Öchslin, 2005)

Der Tag enthält neben einem aktuellen Pseudonym P zwei Sessionnummern: die Nummer der aktuellen Session i sowie die zuletzt erfolgreiche Session i*. Wenn ein Reader eine Leseanforderung an den Tag sendet, so erhöht der Tag die aktuelle Seriennummer i um 1 und sendet hash(P), hash(c(i, P)) – wobei c eine einfache Verknüpfungsfunktion wie etwa XOR ist – und Δ(i):= i – i* an den Reader zurück. Die Backend-Datenbank hat zu jedem Tag hash(P) gespeichert und benutzt diesen Wert als Primärschlüssel, um zusätzliche Informationen zum Tag zu speichern.

Der Wert hash(c(i, P)) soll gegen Replay-Attacken schützen, Δ(i) bewirkt, dass das Backend, das ja die Sessionnummer i* seines letzten Lesevorgangs bei diesem Tag kennt, in der Lage ist, die aktuelle Sessionnummer i zu berechnen, ohne dass Dritte dies können.

Wenn die vom Tag übermittelten Werte gültig sind, so sendet der Reader eine Zufallszahl r und einen weiteren Hashwert hash(c(r, i, P)) zum Tag, der selbst wiederum überprüfen kann, ob dieser Wert korrekt ist. In diesem Fall berechnet er – genau wie das Backend – sein neues Pseudonym P':= c(r, P) und setzt i*=i. Beide Werte werden beim nächsten Identifikationsvorgang verwendet.

Dieses Verfahren muss als unsicher betrachtet werden. Mehrere Angriffe darauf werden in einem Artikel von Avoine / Öchslin vorgestellt.[646] Ein Angreifer könnte z.B. durch viele fehlgeschlagende Leseversuche den Wert i und damit Δ(i) künstlich stark erhöhen, um den Tag mit hoher Wahrscheinlichkeit identifizieren und verfolgen zu können.

---

[645] Henrici / Müller, Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers, 2004; Henrici / Müller, Tackling Security and Privacy Issues in Radio Frequency Identification Devices, 2004.

[646] Avoine / Öchslin, RFID Traceability: A Multilayer Problem, 2005, S. 131-134.

Allgemein eignet sich das Verfahren nur für relativ eng umgrenzte, geschlossene Systeme, da das Backend die Tags bereits vorher kennen und zum erfolgreichen Auslesen alle Reader Zugriff auf die Datenbank erhalten müssen. Ob eine solche Architektur in der Praxis auch in globalen, offenen Systemen skalierbar und sicher arbeiten kann, bleibt zweifelhaft.

7.2.3.2.7.5 Verkettete Hashfunktionen

Ein weiteres Verfahren[647] setzt zwei verschiedene Hashfunktionen, genannt G und H, zur Pseudonymbildung ein, die sowohl dem Tag als auch einem Backend-System bekannt sind. In einem wiederbeschreibbaren Datenbereich des Tags ist zunächst ein Startwert s_1 gespeichert, der sich im Laufe der Zeit ändert. Bei einem Lesezugriff eines Readers berechnet der Tag zwei neue Werte, den externen Wert $a_i = G(s_i)$ sowie den neuen internen Wert $s_{i+1} = H(s_i)$.

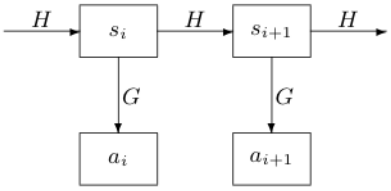


Abbildung 40: Verkettete Hashfunktionen (Okhubo, 2003)

Der Anfangswert s_1 wird zusammen mit der echten Tag-ID im Backend-System gespeichert. Für alle dort gespeicherten IDs berechnet das Backend zu dem jeweiligen Startwert s_1 die Folge von iterierten Hashes $s_i = H^{i-1}(s_1)$ und prüft dann bei jedem Lesezugriff, ob das empfangene $a_i = G(s_i)$ ist. Wenn dies der Fall ist, so kann unter dem Primärschlüssel s_1 die Tag-ID aus der Datenbank ermittelt werden.

Dieses Verfahren ist zunächst nur in geschlossenen, relativ kleinen Systemen anwendbar, wo die Tags und ihre IDs bereits vorher bekannt sind. Es eignet sich unter diesen Voraussetzungen sehr gut, um den wahren Identifikator und Aufenthaltsort des Tags durch die Unumkehrbarkeit der Hashfunktion zu verschleiern.

Voraussetzung ist, dass Tag und Backend gut miteinander synchronisiert sind, was die Anzahl der durchgeführten Leseversuche betrifft. Wenn es durch fremde Reader möglich ist, den Tag viel öfter seinen internen Wert aktualisieren zu lassen als im Backend, wird der Suchaufwand noch viel größer, als er bereits so schon ist – die Berechnung der Hashfolge muss im Backend schließlich für alle IDs erfolgen.

Die Autoren skizzieren eine Ergänzung, um das System mittels des EPC-Netzwerks offener und verteilt zu gestalten; angesichts von Sicherheitslücken im jetzigen Design des EPC-Netzwerks (siehe Kap. 7.2.4.2.1) würde das System damit auch weitere Schwächen erben.

[647] Okhubo / Suzuki / Kinoshita, 2003; 2004; 2005.

7.2.3.2.7.6 „Zero-knowledge“-Verfahren

Beim sogenannten[648] „Zero-knowledge“-Authentifzierungsverfahren[649] führt der Tag-Besitzer ein kleines Gerät, z.B. einen PDA, mit sich, in dem die eigentlichen EPCs seiner Tags gespeichert sind und das als eine Art Verwaltungseinheit fungiert. Auf den Tags muss wiederum eine Hashfunktion zur Verfügung stehen.

Nach dem Kauf wird der Tag in einen „Privacy“-Modus versetzt, in dem er nur noch auf authentifizierte Anfragen von Readern antwortet, anderenfalls aber keinerlei Identifikator preisgibt. Die eigentlichen authentifizierten Anfragen werden vom Nutzer initiiert und von seinem PDA generiert, der sie über einen nicht näher spezifizierten Kanal (der aber nicht RFID nutzt) an den Reader weiterleitet, damit dieser sich beim Tag über den eigentlichen RFID-Kanal authentifizieren kann.

Die Tags enthalten keinen EPC mehr, was auch als Schutz gegen hardwarenahe Auslesevesuche mit Spezialgeräten dient – nur was nicht auf den Tags zu finden ist, kann dort auch garantiert keine Bedrohung der Privatsphäre zur Folge haben.

Ein gemeinsames Geheimnis s zwischen Tag und PDA dient als Grundlage der Authentifikation, wobei im Protokoll auch zwei Einmal-Zufallszahlen m und n benutzt werden. Das Format der Authentifizierungsnachricht des Readers (bzw. Akteurs) an den Tag ist:

Akteur[650] (via Reader) ->Tag: `{m, n XOR hash(m XOR s), hash(n XOR s)}`

Dabei soll m Replay-Attacken verhindern – die Autoren schlagen dafür einen Zeitstempel vor, der allerdings eine Zeitsynchronisation zwischen allen zu autorisierenden Readern voraussetzt – und wird auf dem Tag gespeichert. Der Wert n dient als Sitzungsschlüssel und sollte nur von demjenigen aus der Nachricht ableitbar sein, der neben dem m im Klartext auch den geheimen Schlüssel s kennt. Der letzte Teil der Nachricht dient der eigentlichen Authentifikation.

Der Tag antwortet nur auf authentifizierte Anfragen und gibt andernfalls auch keinerlei Hinweis auf seine Präsenz (und die seines Trägers). Die Antwortnachricht hat folgende Gestalt:

Tag -> Akteur (via Reader): `{hash(n XOR S XOR m)}`

Mit dieser Nachricht kann der Tag sich seinerseits beim Akteur authentifizieren, wiederum ohne Identifikatoren preiszugeben oder solche überhaupt zu kennen.

Positiv zu bewerten ist, dass weder Passwörter noch Pseudonyme noch andere Identifikatoren im Klartext übertragen werden. Tracking und Auslesen des Besitzes über die RFID-Schnittstelle werden so sehr schwierig gemacht. Die Reader selbst müssen nicht vertrauenswürdig sein, die Authentifikationsnachricht wird durch den Akteur generiert und gilt nur für die aktuelle Sitzung, z.B. im Gegensatz zu dem Ansatz, der Readerinfrastruktur selbst ein

[648] Für die Autoren bedeutet dieser Begriff insbesondere, dass kein Identifikator auf den Tags oder im Protokoll vorhanden sein muss.

[649] Engberg / Harning / Jensen, Zero-knowledge Device Authentication, 2004.

[650] Nutzer und PDA zusammen werden in der Arbeit als ein Akteur („actor“) aufgefasst.

Passwort mitzuteilen.

Allerdings stellt sich auch bei diesem Verfahren die Frage nach der Skalierbarkeit und Handhabbarkeit – bei jedem erlaubten Ausleseversuch muss die Nutzerdatenbank (z.B. auf besagtem PDA) verfügbar sein.

Das Problem des Schlüsselmanagements, das sich hier für symmetrische Schlüssel stellt, bleibt ebenfalls erhalten: Benutzt man denselben Schlüssel für mehrere Tags, oder, was sicherer ist, verschiedene? Der ohnehin vorhandene PDA mit seiner Datenbank kann aber den Einsatz verschiedener Schlüssel sehr erleichtern.

Aus multilateraler Sicht ist für die Authentifizierung und den Echtheitsnachweis des Tags problematisch, dass der Identifikator auf dem Tag vom Nutzer frei änderbar ist. An diesem Beispiel zeigt sich ein starker Interessenskonflikt: Wer soll die Kontrolle über am Körper oder im Haushalt eingesetzte Geräte und Information im UC haben?

Aufschlussreich auch für allgemeines UC ist die Diskussion der Autoren, wie in einer permanent überwachten Umgebung (wie einem Supermarkt) Schutzverfahren für RFID mit allgemeiner Privacy-Enhancing-Technology (PET) verbunden werden müssen, um wirksam zu sein:

„Therefore if Security and Privacy are to be maintained when introducing Tags to the pervasive space, we must assume PET is implemented for the consumer. This includes, but is not limited to, Smartcards, Payments, Communication Devices and Surveillance (e.g. Cameras), which should all be designed with security and privacy in mind.“[651]

Dieser Hinweis gilt allgemein. Je stärker das allgemeine Monitoring in UC-Umgebungen ist, desto schwieriger wird in der Praxis der erfolgreiche Einsatz von Schutzmethoden nur für einzelne Technologien. Es kann durchaus möglich sein, dass eine Methode, die für eine bestimmte Technologie Schutz bieten soll, die Verfolgbarkeit und Angreifbarkeit mithilfe einer anderen dazu nötigen Technologie erhöht.[652]

Nach der Diskussion von Lösungen, die darauf abzielen, einen Schutz von Informationssicherheit und informationeller Selbstbestimmung durch technische Maßnahmen und die Kontrolle des Nutzers zu garantieren, werden im Anschluss eher organisatorische Lösungen diskutiert, die von Technik unterstützt werden. Diese Modelle gehen allerdings davon aus, dass alle angebotenen Dienste immer, also z.B. auch nach einem Wechsel des technischen Betreibers, dem Eindringen von schädlicher Software (Malware) oder einem Hacker-Angriff, regelkonform konfiguriert sind, und dass insbesondere keine böswilligen Betreiber auftreten. Da diese Annahme in den offenen Systemen des UC nicht realistisch ist, sind solche Modelle als umfassender Schutz ungeeignet. Sie können aber dennoch als Ergänzung anderer Maßnahmen oder zur technischen Unterstützung z.B. gesetzlicher Anforderungen dienen.

---

[651] Engberg / Harning / Jensen, Zero-knowledge Device Authentication, 2004, S. 7.

[652] Diese Gefahr besteht z.B. in der weiter unten im Kap. 7.2.3.2.8.2 diskutierten Verbindung von RFID und P3P.

7.2.3.2.8 Transparenz und „Fair Information Principles“ für RFID

Neben mehr oder minder überzeugenden Ideen für direkte technische Schutzmaßnahmen gibt es auch Ansätze, die informationelle Selbstbestimmung als freiwillige Selbstverpflichtung von Herstellern und Betreibern von RFID-Systemen einzufordern. Im Geiste von Projekten wie der „Platform for Privacy Preferences“ (P3P)[653] oder EPAL[654] könnte ein Abgleich zwischen den Datenschutzerklärungen (Privacy-Policies) und Nutzerpräferenzen auf UC verallgemeinert und auch dort in gewissem Umfang automatisiert werden.

7.2.3.2.8.1 RFID-„Bill of Rights“

Bereits 2002 formulierte Simson Garfinkel einen griffigen Forderungskatalog zu RFID und der Wahrung der Privatsphäre, die „RFID Bill of Rights“[655]. Als freiwillige Richtlinie soll sie die Rechte der Kunden beim Einsatz von RFID-Systemen formulieren:[656]

1. Das Recht zu wissen, welche Produkte RFID-Tags enthalten.
2. Das Recht, RFID-Tags beim Kauf entfernen oder deaktivieren zu lassen.
3. Das Recht, Dienste, die RFID benutzen, auch ohne RFID-Tags nutzen zu können.
4. Das Recht, auf die in einem RFID-Tag gespeicherten Daten zugreifen zu können.
5. Das Recht zu wissen, wann, wo und warum Tags ausgelesen werden.

Hauptverdienst der „Bill of Rights“ ist ihre recht frühe Entstehung und sehr konzentrierte Formulierung. Besonders der vierte Punkt sollte auf beteiligte Hintergrundsysteme ausgedehnt[657] und um die Forderung nach Datensicherheit ergänzt werden. Ob allerdings ein freiwilliger Selbstverpflichtungsmechanismus den Kunden genügen kann, erscheint zumindest zweifelhaft. Insbesondere, wenn keine entsprechenden Sanktionen die Einhaltung der Selbstverpflichtung begleiten, ist eine massive Nichteinhaltung durch die Betreiber ökonomisch sinnvoll.[658]

7.2.3.2.8.2 „Fair Information Principles“

Eine Idee, wie Datenschutz-Präferenzen von Nutzern von RFID-Systemen beachtet werden können, ist ihre direkte Einbettung in die RFID-Protokolle.[659] Als Grundlage dafür können

---

[653] P3P-Homepage: http://www.w3.org/P3P/ (31.01.2006).

[654] Enterprise Privacy Authorization Language (EPAL): http://www.w3.org/Submission/EPAL/ (02.03.2006).

[655] Garfinkel, RFID Bill of Rights, 2002.

[656] Übers. d. d. Verf.

[657] D.h. das Recht zu wissen, welche Daten mit den Daten auf dem Tag verknüpft sind, wo diese zu welchem Zweck gespeichert sind und wer darauf Zugriff hat.

[658] Bauer / Fabian / Fischmann / Gürses, Emerging Markets for RFID Traces, 2006.

[659] Floerkemeier / Schneider / Langheinrich, Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, 2005.

zum Beispiel die „Fair Information Principles“ (FIP) der OECD[660] dienen, die die folgenden Richtlinien zur Handhabung persönlicher Daten enthalten:

- Beschränkung der Datensammlung (Collection Limitation Principle): Nicht mehr Daten als unbedingt notwendig zur Erfüllung des Zwecks sollen gesammelt werden.
- Datenqualität (Data Quality Principle): Wenn persönliche Daten gespeichert werden, so sollen sie korrekt sein.
- Zwecknennung (Purpose Specification Principle): Der Zweck der Datensammlung sollte zur Zeit der Erhebung genannt werden.
- Beschränkung der Datennutzung (Use Limitation Principle): Nur für den genannten Zweck sollten die Daten genutzt und nicht ohne Einwilligung an Dritte weitergegeben werden – ausgenommen davon ist die Weitergabe nach jeweiligen gesetzlichen Bestimmungen.
- Datensicherheit (Security Safeguards Principle): Die Daten sollten „in vernünftigem Umfang“ vor Verlust, unautorisiertem Zugriff oder Benutzung, Veränderung oder Veröffentlichung geschützt werden.
- Transparenz (Openness Principle): Generell sollte Transparenz vorherrschen, sowohl welche Daten genau gespeichert werden als auch welchen Prozeduren und Richtlinien ihre Verarbeitung unterworfen ist, besonders auch, wer die Daten vorhält und wo er sich befindet.
- Individuelles Auskunftsrecht (Individual Participation Principle): Jedes Individuum sollte das Recht haben, vom Vorhalter der Daten zu erfahren, ob und welche Daten über es gespeichert sind, Widerspruch gegen eine Verweigerung einlegen zu können und die Daten selbst auf Wunsch löschen, korrigieren oder erweitern lassen zu können.
- Verantwortlichkeit (Accountability Principle): Derjenige, der die Daten vorhält (Data Controller), soll für die Einhaltung obiger Prinzipien verantwortlich sein.

Teile dieses Prinzipienkatalogs können durch kleine Modifikationen der bestehenden Standards in die RFID-Protokolle integriert werden, so z.B. die Beschränkung der Datensammlung, Zwecknennung, Transparenz und Verantwortlichkeit.[661] Zu diesem Zweck wird die Einführung einer eindeutigen Reader-Policy-ID (RPID) in den vom Reader gesendeten „Inventory“-Befehl vorgeschlagen, die wiederum drei Teile hat: ID des Datensammlers, eine Policy-ID und eine Reader-ID.

Mithilfe der RPID soll eine informationelle Symmetrie zum EPC hergestellt und gegenseitige Identifikation ermöglicht werden. Anhand dieser Informationen kann dann über einen ande-

[660] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, September 1980. Dort als „Principles“ (Prinzipien) bezeichnet, Exzerpte sprechen auch oft von „Practices“ (d.h. bewährten Praktiken).

[661] Floerkemeier / Schneider / Langheinrich, Scanning with a Purpose – Supporting the Fair Information Principles in RFID protocols, 2005, S. 3.

ren Kanal als RFID wie z.B. WLAN die gesamte Policy aus LAN oder Internet geladen werden. Anhand der Reader-ID wiederum soll man auch den Ort des Auslesevorgangs in Erfahrung bringen können.

Um den unsichtbaren Auslesevorgang mittels RFID wahrnehmbar zu machen, wird der Einsatz eines „Wächter-Tags“ (Watchdog Tag) vorgeschlagen. Dieser Wächter-Tag ist eine Art kleiner PDA, kann aber auch das normale Protokoll für passive RFID-Tags mitlesen.[662] Mithilfe der RPID kann der Wächter Lesevorgänge mit zugehörigen Reader-IDs und Policies anzeigen und protokollieren.

Das Verfahren geht über eine Ankündigung einer Datensammlung – etwa mittels Hinweisen oder Etiketten – insofern weit hinaus, als die Ankündigung und der Zweck der Datenerhebung in das eigentliche RFID-Protokoll integriert und damit in gewisser Weise automatisierbar wird. Allerdings kann durch die Verwendung eines zweiten Kanals (nicht RFID) oder von Internetressourcen, um zu den jeweiligen ID-Nummern die vollständige Policy, Datenerfasser und den Readerstandort herauszufinden, eine Reihe neuer Risiken für die informationelle Selbstbestimmung entstehen.

Wie die Autoren auch selbst anmerken, schützt die vorgeschlagene Protokollerweiterung nicht vor Lesegeräten, die sich nicht an die neue Konvention halten und z.B. keine oder eine falsche RPID übermitteln. Somit wäre in der Praxis eine starke Flankierung durch rechtliche Maßnahmen erforderlich, die natürlich auch spezielle Ausnahmeregeln z.B. für die Strafverfolgung enthalten könnten. Diese Ausnahmeregeln ließen sich dann allerdings nicht nur von Berechtigten, sondern ggf. auch von Angreifern ausnutzen. Das Problem, seine eigenen Privacy-Präferenzen in der Praxis auch garantiert durchsetzen zu können, bleibt bei diesem System offen.

7.2.3.2.9 Trusted Computing in RFID-Readern

Ein anderer Entwurf beinhaltet die Durchsetzung von Privacy Policies mithilfe von Digital Rights Management-Systemen (DRMS)[663] und Trusted Computing.[664] Hierbei soll jeder RFID-Reader ein Trusted Platform Module (TPM) enthalten, das im Gegensatz zum Reader selbst sicher vor Manipulation ist.

Neben der TPM-Komponente soll eine „Policy Engine“ eine Liste mit Tags führen, die ausgelesen werden dürfen, und dabei spezifizieren, welcher Zweck der Datensammlung jeweils erlaubt ist. Außerdem verwaltet die Policy Engine die jeweiligen symmetrischen Schlüssel zwischen Reader und Tag. Ein „Consumer Agent“ bildet die Schnittstelle für die vom Auslesevorgang Betroffenen, um die Einhaltung von Privacy Policies überwachen und durchset-

---

[662] Auf diesem PDA könnte beispielsweise eine Version von der noch in der Entwicklung befindlichen *librfid* und ein RFID-Sniffer wie *rfiddump* laufen. http://rfiddump.org/ (01.02.2006)

[663] Hansen / Möller, Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung, 2005.

[664] Molnar / Soppera / Wagner, Privacy for RFID Through Trusted Computing, 2005. Hansen, Ein zweischneidiges Schwert – Über die Auswirkungen von Trusted Computing auf die Privatsphäre, 2004.

zen zu können. Dies soll weitgehend automatisch geschehen.

Eine globale Privacy-DRM-Infrastruktur könnte auch eine Lösung für das Schlüsselmanagement beinhalten – doch ist sie realistisch, und welche neuen Risiken können durch ihre Existenz und eventuelle Mängel in Implementierung und Handhabung entstehen?

Es ist nicht klar, warum Betreiber von RFID-Systemen ohne gesetzlichen Druck die Kontrolle über die von ihren Readern ausgelesenen Daten abgeben sollten – eine juristische Flankierung oder sehr starke andere Anreize wären notwendig.

Vollkommen unklar ist, wie skalierbar ein solches System bei anvisiertem globalen Einsatz wäre und inwieweit die Überwachung und Durchsetzung von Privacy Policies wirklich gut automatisierbar ist, insbesondere, wenn in unterschiedlichen Regionen unterschiedliche gesetzliche Rahmenbedingungen existieren. Insgesamt wirkt der Vorschlag noch zu unkonkret, um abschließend beurteilt werden zu können.

7.2.3.2.10 Ausblick: Anforderungsanalysen für RFID Privacy-Lösungen

Bei der Betrachtung der verschiedenen Lösungsvorschläge für die Probleme, die RFID-Systeme für die informationelle Selbstbestimmung darstellen, wird deutlich, dass es an einer detaillierten und allgemein akzeptierten Anforderungsanalyse mangelt.

Erste Schritte in diese Richtung könnte z.B. die sogenannte „Privatsphärenschutz-Checkliste“ (Privacy Checklist) der Universität Bielefeld darstellen.[665] Natürlich müssen dazu einige der dort aufgeführten Kriterien präzisiert und auf Vollständigkeit überprüft werden.[666]

Ein anderer Ansatz ist die Formulierung (nur vordergründig einfacher) „Security Policy“-Modelle, um essentielle Minimalanforderungen für Sicherheit und Datenschutz an RFID-Systeme abstrakt zu erfassen.

Ein Beispiel hierfür ist die Idee, dass eine Form des weiter oben diskutierten Resurrecting Duckling-Prinzips Anwendung auf RFID findet, was z.B. auch sein Autor selbst postuliert.[667] In der Form eines „Ownership-based RFID security policy model“ wird als Grundidee die einfache Anforderung beschrieben, dass ein Tag nur von seinem Besitzer ausgelesen werden darf, der zugleich auch Besitzer des mit dem Tag versehenen Objekts sein muss. Wie beim Resurrecting Duckling ist es nicht das Ziel zu beschreiben, was heutzutage mit technischen und kryptographischen Mitteln machbar ist, sondern was das Ideal wäre, wenn bereits geeignete Mittel zur Verfügung ständen. Bei jedem solchen Modell sind allerdings zwei zentrale Fragen zu beantworten:

1. Ist das Modell widerspruchsfrei?

---

[665] Hennig / Ladkin / Sieker, Privacy Enhancing Technology Concepts for RFID Technology Scrutinized, 2004. Sieker / Ladkin / Hennig: Privacy Checklist for Privacy Enhancing Technology Concepts for RFID Technology Revisited, 2005.

[666] Diskussion z.B. bei Berthold / Günther / Spiekermann, Wirtschaftsinformatik 6 (2005), Nr. 47, S. 425f.

[667] Stajano, CACM 48 (9), September 2005, S. 31-33. Ausführlicher: Stajano, RFID is X-Ray Vision, Technical Report, 2005.

2. Gibt es eine realistische Chance, dass dieses Modell jemals in die Praxis umgesetzt werden kann?

Eine wirklich präzise Anforderungsanalyse für RFID-Tags auf privaten Gegenständen, die diversen praktischen Anwendungsszenarien standhält, ist ein offenes Forschungsgebiet.

Ist das Privacy-Enhancing-Technology-Konzept (PET-Konzept) so geartet, dass ...

a. es Datensparsamkeit erzwingt?
b. es auf der Durchsetzung des Daten- und Privatsphärenschutzes als Grundsatz basiert?
c. es dem Bürger die Kontrolle über die Technik überträgt?
d. es das Tag automatisch in einen gesicherten Modus versetzt?[1]
e. es nachweisbar sicherstellt, dass das automatische Versetzen in den gesicherten Modus immer stattfindet?
f. die Kommunikation zwischen Tag und Lesegerät abhörsicher ist?
g. es den Bürger vor dem Hersteller schützt?
h. es den Bürger vor dem Handel schützt?
i. es den Schutz des Bürgers im Laden einschließt?
j. die Anwesenheit eines Tags im gesicherten Modus nicht erkannt werden kann?
k. es keine aktiven Schutzmaßnahmen vom Bürger erfordert?
l. es aktive Schutzmaßnahmen nicht behindert?[2]
m. es die Entstehung und Nutzung zentraler Datenbanken vermeidet?
n. es generell die Entstehung und Nutzung von Datenbanken vermeidet?[3]
o. es die Nutzung von Funktionalität nach dem Kauf in sicherer Weise ermöglicht?[4]
p. es mit bestehender RFID-Technologie umgesetzt werden kann?
q. dadurch die Tag-Kosten nicht erheblich steigen?
r. dadurch die Tag-Kosten gar nicht steigen?
s. dadurch kein weiterer Nachteil für die Privatsphäre entsteht?
t. dadurch eine weiterreichende Verbesserung der Privatsphäre erfolgt?
u. davon der Handel profitiert?

[1] Tags ohne sicheren Modus werden automatisch endgültig deaktiviert („zerstört")
[2] z.B. Benutzung von Blocker-Tags. Aktive Schutzmaßnahmen sind umstritten, dennoch sollte sich aus ihrer Benutzung keine Beeinträchtigung der Schutzwirkung anderer Schutzmaßnahmen ergeben
[3] Datenbanken, die eine Zuordnung zwischen Objekten und Personen, auch indirekt, ermöglichen
[4] z.B. intelligente Kühlschränke und Waschmaschinen

Abbildung 41: RFID Privacy-Checklist (Sieker / Ladkin / Hennig, 2005)

7.2.3.2.11 Zusammenfassung RFID

Die Suche nach Lösungen für Informationssicherheit und informationelle Selbstbestimmung in RFID-Systemen ist ein offenes Forschungsgebiet. Solange Tags mit guter Sicherheitsfunktionalität auf absehbare Zeit zu teuer für den Massenmarkt sind, sollte man unserer Ansicht nach auf den Einsatz von RFID auf Einzelprodukten nach dem Kauf verzichten.

Selbst unter der Voraussetzung, dass auf allen Tags im Privatbesitz eine kryptographische Hashfunktion oder symmetrische Verschlüsselungsverfahren eingesetzt werden könnten, ist die Annahme, dass daraus sofort ein sicheres Gesamtsystem resultiert, falsch.[668]

Für geschlossene Systeme[669] mit vorher bekanntem Teilnehmerkreis und einer begrenzten Anzahl von Tags bietet vor allem das Verfahren der verketteten Hashfunktionen einen recht hohen Schutz vor unerlaubtem Auslesen und Verfolgen durch Dritte, auch das um Challen-

[668] Es bleibt z.B. die Möglichkeit von Side Channel Attacks, siehe die entsprechende Anmerkung im Kap. 7.2.3.2.4, und die Gefahr, Protokolle und Implementation fehlerhaft zu gestalten.

[669] Prinzipiell unklar ist, ob Radio-Systeme überhaupt als geschlossene Systeme aufgefasst werden können.

ge-Response erweiterte Passwortmodell könnte umsetzbar sein. Alle Verfahren müssten allerdings um ein sicheres Verfahren zum Schlüsselmanagement ergänzt werden – ein Problem, das noch nicht einmal theoretisch gelöst ist. Außerdem sind alle Verfahren ungeeignet, die erst oberhalb der Sicherungsschicht ansetzen und die Identifikatoren für die Antikollisionsprotokolle unverändert lassen, da sie ein Tracking und ein Auslesen des Besitzes nicht verhindern.

Das vorgestellte Zero-knowledge-Verfahren scheint auch für größere und offene Systeme einsetzbar zu sein, das erweiterte Passwortmodell hingegen hinterlässt in jedem einmal autorisierten Reader das Originalpasswort; hier könnte, um Sicherheit durchzusetzen, nur der Vorschlag einer Trusted-Computing-Architektur die Passwörter sichern, deren praktische Umsetzbarkeit aber höchst unwahrscheinlich erscheint. Auch das Zero-Knowledge-Verfahren benötigt ein Tag-externes Passwortmanagement, etwa auf dem bereits im Verfahren beschriebenem PDA.

Die vielen Kommunikationsprotokolle und Applikationen auf einem derartigen Master-Gerät[670] könnten jedoch leicht neue, über das Internet ausnutzbare Verwundbarkeiten schaffen. So könnten Trojanische Pferde oder ähnliche „Malware“ die gesamte Passwortdatenbank des Nutzers „ernten“ und über das Internet versenden.

Ohne einfache, d.h. vom normalen Nutzer durchführbare Verfahren zum Rückruf von Schlüsseln in den Tags sind somit alle betrachteten Lösungen nicht dauerhaft sicher. Überhaupt dürfen Nutzer nicht von den Verfahren zum Schutz ihrer Privatsphäre überfordert werden, sonst werden „störende“ Faktoren – wie z.B. das Benutzen verschiedener Passwörter – ignoriert, und das System versagt.

Ansätze zur Selbstverpflichtung, Datenschutzrichtlinien (Privacy Policies) einzuhalten, sind selbst dann, wenn sie mit starken gesetzlichen Verpflichtungen flankiert werden, nicht sicher; insbesondere die Unauffälligkeit des Zugriffs über eine Funkschnittstelle bietet zu viele heimliche Gelegenheiten, Daten zur Profilierung zu sammeln.

Schließlich bleibt bei allen Verfahren die Möglichkeit, dass Information, die einem autorisierten Dienstanbieter zur Verfügung gestellt wird, von ihm missbraucht oder (auch unfreiwillig durch Angriffe auf sein Datenverarbeitungssystem) an Dritte weitergeleitet werden kann. Besteht zur Datenweitergabe sogar eine gesetzliche Verpflichtung, z.B. zur Überwachung öffentlicher Räume, so kann kein Verfahren, das Tags nach dem Kauf verwendbar lässt, davor schützen.

Das Problem der Informationssicherheit und des Schutzes der Privatsphäre in RFID-gestützten UC-Umgebungen ist daher als ungelöst zu betrachten. Solange das Paradigma der Kostenminimierung bei den Tags dominiert, erscheint es ferner höchst zweifelhaft, ob eine befriedigende Lösung denkbar und für die Zukunft zu erwarten ist.

[670] An einem solchen Gerät, das neben dem Management von Userpasswörtern auch RFID-Relay und partielles Blocken beherrschen soll, wird im Projekt RFID Guardian geforscht: Rieback / Crispo / Tanenbaum, 2005; RFID Guardian Homepage http://www.rfidguardian.org/ (17.03.2006).

7.2.3.3 Informationssicherheit in Sensor- und Ad-hoc-Netzen

Voraussetzung für adaptive UC-Systeme, die sich an die Zustände von Nutzer und räumlicher Umgebung anpassen können, ist die Erfassung der physischen Umwelt. Seien es Anwendungen wie ein Smart Home mit einem selbsttätig bestellenden Kühlschrank, eine automatische Geschwindigkeitskontrolle für Fahrzeuge oder die vollautomatische Überwachung einer Produktionsstätte – stets ist die Messung eines Zustands Voraussetzung des Systembetriebs. Netzwerke aus Sensoren werden somit einen zentralen Bestandteil vieler UC-Systeme bilden.

Auch wenn im Moment die RFID- und Sensornetzforschung im akademischen Bereich erstaunlich wenig Überschneidungen zeigen, kann man davon ausgehen, dass diese beiden Fachgebiete mittelfristig in der Praxis sehr stark verbunden werden, besonders, wenn neben passiven RFID-Tags auch stärkere Tags mit eigener Energieversorgung zum Einsatz kommen. Viele der Sicherheitsfragen in Sensornetzen können somit auch für RFID-Systeme höchst relevant werden.

Ein Hauptunterschied zwischen RFID-Anwendungen und Sensornetzen besteht im Umfang der übertragenen Daten. Während bei RFID mit einfachen Tags nicht mehr als ein Identifikator übertragen wird, müssen Sensornetze je nach Anwendung und Art der gemessenen Daten (z.B. Schwingungen, Luftfeuchtigkeit, Audiosignale, Videobilder) fähig sein, auch größere Datenmengen, eventuell mit hoher Frequenz, an eine sogenannte Datensenke zu übertragen, die über ein angebundenes klassisches Netzwerk den Kontakt zum eigentlichen Aggregations- und Speicherpunkt der Daten, z.B. einer größeren Datenbank, herstellt.

Das eigentliche Sensornetzwerk kann ein geschlossenes System mit vorher bekannten Teilnehmern sein, ein Ad-hoc-Netzwerk sein oder eine Hybridform besitzen. Offenheit oder Geschlossenheit eines Sensornetzes hat, wie bei RFID, starken Einfluss auf die möglichen Sicherheitsmaßnahmen. Auch ist der Ort ihres Betriebs zu berücksichtigen. Sensornetze, die z.B. in abgeschotteten (automatisierte Fabrik) oder menschenleeren (z.B. Habitat-Monitoring in der Tierverhaltensforschung) Umgebungen betrieben werden, könnten zwar Sicherheitsprobleme aufweisen, doch diese werden sich ebenso wenig wie der Einsatz von RFID auf Paletten in der Logistik auf die informationelle Selbstbestimmung von Menschen auswirken.

Anders sieht es mit Sensorsystemen aus, die in Gegenwart von Menschen betrieben werden, sei es, dass sie explizit zur Unterstützung der Mensch-Maschine-Interaktion in einem UC-System wie einem Smart Home oder zum Überwachen von Patienten eingesetzt werden, sei es, dass sie, z.B. als Erweiterung klassischer Videokameras, zum permanenten Monitoring von öffentlichen Arealen dienen, in denen sich Menschen bewegen. Letztere stellen per se einen starken Eingriff in die informationelle Selbstbestimmung des Individuums dar. Es ist daher besonders die zuerst genannte Kategorie von Anwendungen, bei der Nutzer ihrer eigenen Überwachung auch in sensiblen Bereichen für einen konkreten Zweck zustimmen, wo Informationssicherheit die Wahrung von leiblicher Sicherheit und Selbstbestimmung des Individuums unterstützt.

Ad-hoc-Netze können nicht nur bei der Vernetzung von Sensorknoten entstehen, sondern sind geradezu charakteristisch für viele Visionen des UC, wo etwa spontane Interaktion von

Geräten in und zwischen PANs, Fahrzeugen und der lokalen Umgebung möglich wird.

7.2.3.3.1 Sicherheitsprobleme in Sensor- und Ad-hoc-Netzen

Nahezu alle Sicherheitsprobleme, die in klassischen Netzwerken und verteilten Systemen vorkommen, finden sich auch in Sensor- und Ad-hoc-Netzen[671] wieder, so zum Beispiel das Problem, sensible Daten nicht im Klartext zu übertragen (Vertraulichkeit), sie gegen Verfälschung zu schützen (Integrität) und sicherzustellen, dass Nachricht und „Gesprächspartner" echt sind (Authentizität). Verfügbarkeit, ob gegen natürlich vorkommende Ausfälle oder Denial-of-Service-Angriffe, muss ebenfalls gewährleistet werden.

Im Unterschied zu klassischen Netzwerken – und hier zeigt sich eine starke Parallele zu RFID – gibt es einige neue Rahmenbedingungen, die eine Absicherung von Sensornetzen erschweren. Dazu zählen die Beschränkungen der Hardware (CPU, Speicher) und das Problem der meist mangelnden Energieversorgung, das auch beim Design von Sicherheitsprotokollen berücksichtigt werden muss. Drahtlose Übertragung via Funk erleichtert wie bei WLAN, Bluetooth oder RFID das unauffällige Abhören oder Stören der Kommunikation, und eine mangelnde physische Absicherung kann das direkte Auslesen von kryptographischen Schlüsseln nur schlecht verhindern, zumal die Sensorknoten meist unbewacht sind und nur aus der Ferne gewartet werden.

Abzuwarten bleibt, in wie vielen praktischen UC-Anwendungsbereichen theoretische Anforderungen wie die Fähigkeit zur Ad-hoc-Vernetzung oder Multi-Hop-Routing zentral werden. Dazu zählt auch die Anforderung, generell auf zentrale, ausgezeichnete Serviceknoten und die Verteilung von Diensten auf alle Knoten im Netzwerk zum Zwecke der Redundanz zu verzichten. Alle Verfahren, die derartige Probleme lösen wollen, müssen natürlich wiederum auf ihre Sicherheit überprüft werden – ein noch vollkommen offener Forschungsbereich.

Ein zentrales Problem bei der Absicherung echter Ad-hoc-Netze[672] ist die Notwendigkeit einer möglichst konstanten digitalen Identität[673], mit der Schlüssel und Zertifikate verknüpft werden können. Diese Anforderung steht auch in starkem Gegensatz zur informationellen Selbstbestimmung, denn eine solche Identität, etwa in Form einer globalen PKI, kann sehr leicht zu Profiling und Überwachung benutzt werden.[674]

Noch unklar bleibt, ob hier Pseudonymisierung[675] und ein datenschutzfreundliches Identitätsmanagement (IDM) einen Ausweg aufzeigen können. Wiederum werden mit hoher Wahrscheinlichkeit durch ein solches komplexes System neue Schwachstellen entstehen.

---

[671] Überblick zur Sicherheit in Sensor- und Ad-hoc-Netzwerken z.B. bei Walters et al., Survey, 2006; Blaß / Fabian / Fischmann / Gürses, 2006.

[672] Überblick bei Zhou, 2003; Kargl, Dissertation, Ulm, 2003.

[673] Vgl. Kargl, Dissertation, Ulm, 2003, S. 114ff.

[674] Lösungsansätze dafür sind Protokolle wie Direct Anonymous Attestation, das auch Teil der Trusted Computing-Spezifikationen ist, siehe Brickell / Camenisch / Chen, 2004.

[675] Ibid., S. 135ff.

7.2.3.3.2 Kryptographie auf Sensorknoten

Auch wenn die heutzutage im Allgemeinen leistungsschwache Hardware bei Sensorknoten[676] sicherlich gute Fortschritte machen wird, bleibt ihre Leistungsfähigkeit auf absehbare Zeit durch Platzbedarf und Energieverbrauch beschränkt. Im Gegensatz zu RFID-Tags mit massenmarktfähigen Kosten gibt es allerdings bereits heute verschiedene Implementierungen von symmetrischen Verfahren auf Sensorknoten sowie erste Ansätze von asymmetrischer Kryptographie.[677] Dies ist jedoch nicht ausreichend, man benötigt zusätzlich genügend Speicher für Schlüsselmaterial, Zertifikate und Zufallswerte, die in kryptographischen Protokollen verwendet werden.

7.2.3.3.3 Schlüsselmanagement in Sensor- und Ad-hoc-Netzen

Das zentrale Problem ist auch bei Sensor- und Ad-hoc-Netzen das Schlüsselmanagement: Wie können die Schlüssel oder Zertifikate sicher verteilt, geändert und zurückgerufen werden? Die naive Idee, für alle beteiligten Geräte denselben Schlüssel zu benutzen, riskiert die Sicherheit des Gesamtnetzes, sobald nur einmal ein Schlüssel einem Angreifer bekannt wird, z.B., wenn dieser physischen Zugang zu der im Allgemeinen nicht gesicherten Hardware eines einzigen Knoten erhält.

Zwei grundsätzliche Verfahren – neben unzähligen Abwandlungen – für das Management von symmetrischen Schlüsseln in Sensornetzen wurden vorgeschlagen. Der eine Ansatz ist, alle gemeinsamen Schlüssel vor der Installation bereits zwischen den Knoten zu verteilen. Für größere Netzwerke skaliert diese Lösung schlecht, deshalb wurden Verfahren entwickelt, nur Teile der gesamten Schlüsselmenge des Netzwerks auf die jeweiligen Knoten zu verteilen, so dass nach der Installation noch eine sehr hohe Wahrscheinlichkeit besteht, dass je zwei Kommunikationspartner einen Schlüssel gemeinsam haben.[678] Verfeinerungen benutzen andere Knoten als temporäre Vermittler, um dann einen neuen gemeinsamen Schlüssel auszuhandeln.[679]

Von einem schwächeren Angreifermodell geht der zweite Ansatz[680] aus: Hier werden die Schlüssel in den ersten Sekunden nach einer Installation des Sensornetzes am Einsatzort im Klartext ausgetauscht. Wenn ein Angreifer dort keine Abhörinfrastruktur, z.B. ein eigenes Sensornetz, in Bereitschaft hat, kann der Schlüsselaustausch wegen seiner engen räumlichen und zeitlichen Begrenzung unbelauscht vonstatten gehen. Bei zunehmender Verbreitung von UC-Systemen mit untereinander kompatiblen Sensoren könnte langfristig – zumin-

[676] Siehe z.B. http://www.tinyos.net/scoop/special/hardware/ (31.01.2006).

[677] Vgl. z.B. Gupta et al., Sizzle – a standards-based end-to-end security architecture for the embedded Internet, PerCom 2005, S. 247–256; Blaß / Zitterbart, Acceptable Public-Key Encryption in Sensor Networks, 2005.

[678] Eschenauer / Gligor, A key-management scheme for distributed sensor networks, 2002.

[679] So z.B. PIKE: Chan / Perrig, IEEE Infocom, 2005.

[680] Anderson / Chan / Perrig, Key infection: Smart trust for smart dust, ICNP 2004.

dest in besiedelten Gebieten – diese Voraussetzung zunehmend nicht mehr erfüllt sein.[681]

Beim Nutzen von asymmetrischer Kryptographie stellt sich ein analoges Problem zum Verteilen symmetrischer Schlüssel: Wie kann gewährleistet werden, dass ein gegebener öffentlicher Schlüssel auch wirklich zum Empfänger der Nachrichten gehört oder nicht zu jemand anderem, der sich als ein „Man-in-the-middle" in die Kommunikation einzuschleichen versucht?

Zur Lösung gibt es zunächst Vorschläge, eine im Netzwerk genutzte Identität oder Adresse zuverlässig mit einem öffentlichen Schlüssel zu verknüpfen. Bei kryptographisch generierten Identitäten[682] wird aus einem öffentlichen Schlüssel eine eindeutige Hostadresse generiert, die damit aber nicht mehr vollkommen frei konfigurierbar ist. Bei identitätsbasierter Kryptographie[683] geht man den umgekehrten Weg und generiert mithilfe eines vertrauenswürdigen Dritten aus einer Hostadresse einen öffentlichen Schlüssel. Die Notwendigkeit, einem Dritten zu vertrauen und ihn wenn nötig auch erreichen zu können, lässt diesen Ansatz allerdings weniger flexibel erscheinen.

Dem Grundprinzip, aus Gründen der Redundanz Netzwerkdienste möglichst zu verteilen, folgt der Ansatz der verteilten Certificate Authority (CA).[684] Statt eine einzelne CA wie in klassischen Netzen zu verwenden, teilt sich eine bestimmte Anzahl von Knoten diese Funktion. Ein Teil dieser Knoten darf sogar ausfallen oder kompromittiert werden, ohne die Funktion und Sicherheit der Schlüsselverteilung zu gefährden. Dieses Verfahren ist aber nicht besonders flexibel bei großen Fluktuationen in der Teilnehmerschaft des Netzes.

Schließlich gibt es noch den Ansatz[685], das sogenannte „Web of Trust" von „Pretty Good Privacy" (PGP)[686] auf Ad-hoc-Netze zu übertragen. Hier gibt es keinerlei zentrale Instanz, sondern die Teilnehmer selbst stellen einander Zertifikate aus, so dass mit der Zeit ein „Vertrauensgraph" entsteht. So bilden sich mit recht hoher Wahrscheinlichkeit Vertrauensketten zwischen den Teilnehmern, aus denen sich beglaubigte öffentliche Schlüssel zur Kommunikation ergeben.

Nachteile des Verfahren sind seine Anfälligkeit gegenüber nachlässigen oder unehrlichen Nutzern, die falsche Zertifikate ausstellen, sein lediglich heuristischer Ansatz, der keine Vertrauenskette garantieren kann, sowie die Notwendigkeit, Vertrauensbeziehungen, die ja recht genau soziale Beziehungen widerspiegeln können, für jeden Teilnehmer im Netz öffentlich zu machen.

---

[681] Anwendungsparadigma dieses Ansatzes ist eigentlich die „Ausstreuung" eines militärischen Sensornetzwerks wie „Smart Dust" in mehr oder minder freiem Gelände.

[682] Bobba et al., Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks, 2002. Seinen Ursprung hat die Idee in der Absicherung von MIPv6, siehe Soliman, 2004, S. 142 – 144.

[683] Khalili / Katz / Arbaugh, Toward Secure Key Distribution in Truly Ad-Hoc Networks, 2003.

[684] Zhou / Haas, IEEE Network 6 (13), 1999, S. 24–30.

[685] Hubaux / Buttyán / Capkun: The Quest for Security in Mobile Ad Hoc Networks, 2001.

[686] PGP Homepage: http://www.pgpi.org/ (01.02.2006).

7.2.3.3.4 Zusammenfassung

Sicherheit in Sensor- und Ad-hoc-Netzen ist ein sehr aktives Forschungsgebiet. Neuartige Probleme sind insbesondere die physische Verwundbarkeit dieser verteilten Systeme und das massive Ungleichgewicht in der Rechenfähigkeit zwischen Sensorknoten oder mobilem Kleinstgerät und einem vollwertigen Laptop eines Angreifers.

Für geschlossene Netze mit bekannten Teilnehmern gibt es recht gute theoretische Verfahren zum Schlüsselmanagement, die allerdings auch noch intensiv in der Praxis erprobt werden müssen.

Betrachtet man allerdings offene Systeme und echte Ad-hoc-Netze, an denen auch vorher Unbekannte teilnehmen dürfen (was in fortgeschrittenen UC-Umgebungen oft der Fall sein kann), so ist schon das Grundproblem der digitalen Identität offen. Umso problematischer ist ein darauf aufbauendes Schlüsselmanagement, das neben der sicheren Verteilung auch den Rückruf von Zertifikaten umfassen muss und dabei die informationelle Selbstbestimmung des Individuums wahrt.

7.2.4 Informationssicherheit in gekoppelten Internet-Systemen

Mit dem Schutz von autorisiert und regulär erhobenen Daten in der lokalen Infrastruktur, wie etwa Tag-Reader-Systemen bei RFID oder der lokalen Kommunikation von Sensornetzen, endet die Problematik der Informationssicherheit und informationellen Selbstbestimmung nicht. Im Gegenteil, bei immer stärkerer Anbindung von ursprünglich geschlossenen Systemen ans Internet, so etwa zur Interoperabilität bei Informationsübertragung, -beschaffung oder Servicebereitstellung, wachsen auch die Risiken in dem nunmehr offenen Gesamtsystem.

Zunächst behandeln wir die Auswirkungen zunehmender Adressier- und damit Ansprechbarkeit von lokalen Geräten aus der Ferne und gehen dann auf Risiken der Nutzung von mit lokalen UC-Systemen gekoppelten Internetdiensten anhand des Beispiels des EPC-Netzwerks ein.

Im Anschluss geben wir einen Überblick über einige mögliche Lösungen, wobei wir uns besonders auf die Anonymität der Dienstnutzung konzentrieren. Die anderen Sicherheitseigenschaften sind nicht weniger wichtig, fallen aber eher in den Bereich der klassischen IT-Sicherheit, den wir in dieser Studie nicht ausführlich behandeln können.[687]

7.2.4.1 Risiken durch direkte Adressierbarkeit aus der Ferne

Theoretisch besteht kein entscheidendes Hindernis, hunderte von Geräten pro Nutzer zum Beispiel in Form von extensiven Body-Area-Networks aus Sensoren und aktiven Tags mit dem Internet zu verbinden.

[687] Einführungen z.B. bei Stallings, 2002; Eckert, 2004; Bless et al., 2005.

Adressknappheit jedenfalls wird mit zunehmender Verbreitung von IPv6 kein Problem mehr darstellen. Auch wenn der Wechsel von IPv4 global gesehen noch sehr schleppend vorangeht, könnte die Vernetzung von Geräten im UC die nötige Initialzündung sein, damit die Nutzung von IPv6 nach Überschreiten einer kritischen Masse zum Selbstläufer wird.

Haupttreiber könnte ebenfalls das erleichterte Roaming zwischen verschiedenen Accesstechnologien und Providern sein, das die von Mobile IPv6 (MIPv6)[688] bereitgestellte feste und dauerhafte IP-Adresse ermöglicht.

Die Flexibilität und Vorteile einer IP-Vernetzung als allgemeiner Basis für einheitliche Netzwerke, die sich für beliebige Anwendungen nutzen lassen, äußern sich in der fortschreitenden Konvergenz von anderen Netztechnologien (z.B. Telefonie, Audiostreams, Video). Es ist sehr wahrscheinlich, dass bei zunehmender Komplexität und Funktionalität in den Endgeräten[689] auch die Notwendigkeit des Zugangs zum Internet wächst, z.B. zur Informationsbeschaffung, für Updates oder – auch das ein möglicher Treiber – zum Kontakt mit externen Servern, z.B. für DRM.

Andererseits sind auch diverse Dienste denkbar, die einen netzbasierten Fernzugriff auf die Geräte notwendig machen, wie interaktive Wartung, Schulungen oder Monitoring von Gesundheitssensoren. Solche Zugriffe von außen sind viel leichter möglich, wenn Geräte eine dauerhafte Adresse besitzen, auch wenn sie oft zwischen verschiedenen Aufenthaltsorten unterwegs sind – noch eine weitere Motivation zur Nutzung von MIPv6. Die Möglichkeit eines Zugriffs von außen bedeutet aus technischer Sicht nichts anderes, als dass das Gerät unter seiner IP-Adresse Dienste anbietet.

Was bedeutet entfernte Adressierbarkeit von Geräten im UC für die Informationssicherheit? Vereinfacht gesprochen, viele Angriffe auf UC-Systeme müssen nicht mehr lokal ausgeführt werden, sondern könnten bequem und automatisiert aus der Ferne ablaufen, ohne die Gefahr einer Strafverfolgung. Extrapoliert man – in einer rein intuitiven und qualitativen Schätzung – die heutige Verwundbarkeit von Rechnersystemen auf die Geräte allgegenwärtiger Rechnerumgebungen, so ist äußerste Skepsis angebracht, wie sicher UC überhaupt sein kann, wenn sich nicht fundamentale Änderungen in der Praxis der Softwareentwicklung ergeben.

Die Schreckensvision von Wurmverbreitung in Body-Area-Networks, von durch Fremde gesteuerten Sensoren und Aktoren nach der automatischen Ausführung von Exploits gegen Betriebssysteme und Dienste der Kleinstgeräte liegt nahe und ist ohne konsequentes Sicherheitsbewusstsein in Design, Implementierung und Nutzung des UC realistisch.

[688] Überblick bei Soliman, 2004.

[689] Beispielsweise Tags, Sensoren, Aktoren, PDAs, Smart Phones, persönliche Mediacenter und UC-Kommunikatoren jeder Art.

7.2.4.2 Indirekte Angriffsmöglichkeiten

Auch wenn die Geräte des UC nicht über einen IP-Stack[690] verfügen sollten oder nicht mit dem Internet verbunden sind, können indirekte Angriffsmöglichkeiten auf die Informationssicherheit bestehen, indem Schwächen von gekoppelten mit dem Internet verbundenen Informationssystemen ausgenutzt werden.

Falls zum Beispiel die Bereitstellung eines Dienstes im lokalen System zur Informationsbeschaffung auf Server im Internet zugreifen muss, können diverse Logfile-Einträge entstehen, die – vor allem bei langfristiger Speicherung von Verbindungsdaten – wichtige Bausteine für Profiling oder Data Mining bilden können. Als wichtiges Beispiel für ein Internetsystem, das die Informationsbeschaffung zu Objekten mit RFID-Tags vereinheitlichen soll, dient das EPC-Netzwerk.

Danach folgt ein Beipiel, wie mithilfe von RFID-Tags die an ein Reader-System gekoppelten Datenbanken angegriffen werden können.

7.2.4.2.1 Beispiel EPC-Netzwerk

Das von EPCglobal, einem großen internationalen Standardisierungskonsortium, entworfene EPC-Netzwerk soll die globale Anlaufstelle für Objektdaten werden, die nicht auf den Tags selbst, sondern mithilfe von Internet-Diensten durch viele verschiedene Parteien (z.B. Hersteller, Vertriebspartner, andere Informationsanbieter) bereitgestellt werden. Es ist abzusehen, dass nach einer etwaigen Etablierung in vielen Wertschöpfungsketten auch private Anwendungen wie Smart Homes das EPC-Netzwerk nutzen werden, um Informationen über Objekte einzuholen. Die Grundidee ist, auf jedem Tag eine weltweit eindeutige und strukturierte Identifikationsnummer zu speichern, den Electronic Product Code (EPC). Dieser identifiziert nicht nur wie der Barcode die Art des Gegenstandes, sondern jedes einzelne Exemplar derselben Art wird unterschieden.

Den Ablauf der Informationsbeschaffung mithilfe des EPC-Netzwerks zeigt Abbildung 42. Nachdem im ersten Schritt ein Reader den EPC mittels RFID vom Tag gelesen hat, findet im zweiten Schritt mithilfe des Object Name Service (ONS) eine Lokalisierung von Informationsquellen im Internet statt, die dann im dritten Schritt direkt angesprochen werden.

[690] Ein IP-Stack kann es einem Gerät z.B. als Teil des Betriebssystems ermöglichen, eine Internet-Protokoll-Adresse zu verwenden und am Routing im Internet teilzunehmen.

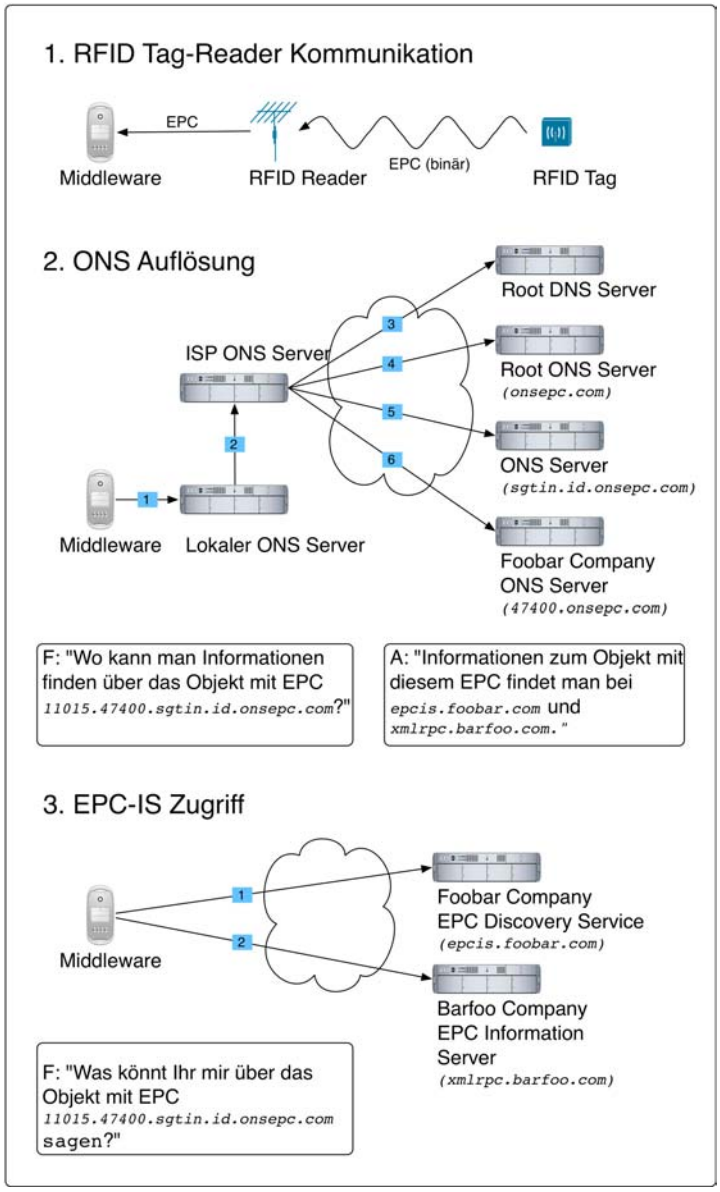


Abbildung 42: Das EPC-Netzwerk (Fabian et al., 2005)

In der bisher von EPCglobal veröffentlichten Struktur zeigen sich bereits einige gravierende Mängel aus Sicht der Informationssicherheit. Besonders der Suchdienst ONS, der im wesentlichen auf dem betagten Domain Name System (DNS) basiert. ONS erbt diverse Schwachstellen dieses klassischen und (entsprechend dem ursprünglich geplanten, vertrauten Teilnehmerkreis) noch ohne Berücksichtigung von IT-Sicherheit entworfenen und oft fehlerhaft implementierten Internet-Dienstes.[691]

Beim ONS wird ein EPC eines Objektes, zu dem mehr Informationen eingeholt werden sollen, nach bestimmten Regeln strukturerhaltend[692] in einen klassischen Domänennamen

[691] Siehe Fabian / Günther / Spiekermann, 2005.

[692] Bisher ohne die Seriennummer, wobei dies aber als zukünftige Option explizit nicht ausgeschlossen wird.

(Domain Name) des DNS übersetzt.[693] Danach wird dieser partielle EPC, an dem man mindestens noch Hersteller und Objektklasse eines Gegenstands ablesen kann, im Klartext, wie bei DNS üblich, durch die gesamte zuständige ONS Hierarchie weitergegeben, insbesondere auch durch sämtliche Router auf dem Kommunikationsweg. Jeder ONS Server auf dem Weg kann den EPC, seine Quell-IP und die Zugriffszeit protokollieren.

Die Zuordnung von IP-Adresse zu einer Identität, sei es Privatperson, Firma oder anderer Organisation ist im bestehenden Internet oft einfach und wird mit zunehmender Verbreitung von IPv6 und insbesondere Mobile IP, das feste Adressen trotz häufigem Zugangsnetz-Wechsel ermöglicht, noch leichter fallen.

Aber auch hinter scheinbar anonymisierenden Maßnahmen wie Network Address Translation (NAT), das ursprünglich den privat verwendbaren Adressraum vergrößern sollte, können einzelne Rechner eindeutig unterschieden werden.[694]

Mit einfachem DNS ist keine überzeugende Überprüfung der Datenintegrität und Authentizität von Nachricht und Absender möglich – somit können sowohl die übertragenen Nachrichten als auch die auf entsprechenden Servern gespeicherten Daten unbemerkt verfälscht werden. DNSSEC ist hierfür eine mögliche Lösung, aber explizit nicht für die Vertraulichkeit der Daten. [695] Unklar bleibt, wie skalierbar DNSSEC wirklich außerhalb geschlossener Systeme ist. Die bisher geringe Verbreitung in der Praxis lässt Skepsis angebracht erscheinen.

Somit könnten zu angefragten EPCs fehlerhafte oder bewusst gefälschte Adressen von Informationsquellen (EPC-IS) zurückgeliefert werden, was je nach Anwendung zu Denial-of-Service- oder raffinierteren Angriffen auf UC-Systeme führen kann, die das EPC-Netzwerk benutzen.

Wenn sich das EPC-Netzwerk in der jetzigen Form als Informationsmedium für globale Supply-Chains etabliert, so ist es sehr wahrscheinlich, dass auch für UC-Anwendungen in privaten Haushalten auf die dann bereits etablierte Infrastruktur zurückgegriffen wird.

Umso wichtiger wäre ein bereits vom Design her überzeugender Entwurf, der bereits im Lookup-Service Sicherheit und Datenschutz berücksichtigt, da nachträgliche „Add-ons“ grundlegende Designschwächen auf diesen Gebieten nicht oder nur mit unrealistisch hohem Aufwand mildern können.

7.2.4.2.2 RFID-Tags als Medien für Angriffe auf Reader und Backend

Mithilfe von auf manipulierten RFID-Tags gespeicherten Daten lassen sich Schwächen in gekoppelten Systemen ausnutzen.[696] Beispiel hierfür ist die mögliche Ausnutzung von (potentiell überall vorhandenen) Programmierfehlern in der Reader- oder Backend-Software

[693] In der aktuellen Spezifikation wird die Seriennummer des EPC nicht zur Delegation benutzt, diese Möglichkeit wird aber explizit für die Zukunft offen gehalten.

[694] Grundlegend z.B. zum Fingerprinting von Computern im Internet: Kohno / Broido / Claffy, 2005, S. 93–108.

[695] Arends et al., RFC 4033, S. 8, S. 15.

[696] Rieback / Crispo / Tanenbaum, Is your Cat infected with a Computer Virus?, PerCom 2006.

mittels Buffer-Overflows[697], wenn der Input von Daten, die von einem nur scheinbar vertrauenswürdigen Tag stammen, nicht sorgfältig auf ihre korrekte Länge und Formatierung überprüft werden.

Auch das Einschleusen von Shell- oder SQL-Code (SQL-Injection), d.h. Code, der unbemerkt in scheinbaren Nutzdaten transportiert, dann aber in Hintergrundsystemen wie einer Datenbank interpretiert und ausgeführt wird, ist ein durchaus ernst zu nehmendes Sicherheitsrisiko analog zu den zahlreichen existierenden Angriffen auf Datenbanken, die mit Webservern verbunden sind.

Solche Angriffe könnten dort auch Befehle ausführen, die den Angriffscode wieder auf andere Tags zurückschreiben lassen, die dann ihrerseits weitere Systeme attackieren könnten. Im Vergleich zu einer Verbreitung über das Internet wäre dies aber um Größenordnungen langsamer, da die Tags erst wieder von (ahnungslosen) Dritten zu Readern mit anfälligen Datenbanken transportiert werden müssten, was die Reaktionszeit, die für Gegenmaßnahmen zur Verfügung steht, erhöht – zumindest, solange Reader nicht allgegenwärtig sind. Echte RFID-Viren oder RFID-Würmer hingegen, die sich direkt zwischen RFID-Tags verbreiten könnten, sind erst für aktive Tags mit höherer Leistungsfähigkeit zu erwarten.

7.2.4.3 Lösungen für Anonymität

Wie bereits angekündigt, konzentrieren wir uns nun in diesem Abschnitt auf einige Lösungen, die Anonymität als Vertraulichkeit der Identität bei der Nutzung von an lokale UC-Systeme gekoppelten Internetsystemen unterstützen können. Dazu zählen unter anderem Private Information Retrieval, die allgemeine Anonymisierung beliebiger Internet-Kommunikation mittels Mix-Verfahren sowie der Einsatz von Peer-to-Peer-Systemen.

7.2.4.3.1 Private Information Retrieval (PIR)

Im UC wird die Anzahl von Daten- und Datenbanken, die Informationen zur Bereitstellung von Diensten in „Intelligenten Umgebungen“ liefern, stark zunehmen. Umso wichtiger werden Methoden, die einerseits Daten verschlüsselt vorhalten und übertragen, andererseits den Zugriff auf diese Daten anonymisieren: Je weniger darüber bekannt ist, wer, wann, wo und zu welchem Zweck auf bestimmte Datensätze zugreift, desto schwieriger wird ein allumfassendes Profiling.

Unter dem allgemeinen Begriff „Private Information Retrieval“ sind verschiedene Verfahren zusammengefasst worden, die unterschiedliche Hauptziele verfolgen. So kann man unterscheiden, ob die Datensätze selbst vom Serviceprovider bereitgestellt oder eingesehen werden können, aber der Zugriff auf die Daten möglichst anonym gestaltet wird,[698] oder ob auch die Daten selbst vor dem Besitzer der Datenbank geschützt werden sollen.

---

[697] Wenn Inputdaten länger sind als vorhergesehen und dies nicht überprüft wird, können ausführbare Anweisungen, die von einem Angreifer stammen, im Arbeitsspeicher eines Computers platziert werden.

[698] Überblick bei Iliev / Smith, 2005, S. 22.

Einige Ansätze sehen den Einsatz eines Trusted-Computing-Moduls in Form eines sicheren Coprozessors zwischen Client und Datenbankserver vor, das weder vom Datenbankbetreiber noch einem anderen Angreifer kontrolliert werden kann.[699] Dazu ist Hardware nötig, die möglichst vielen physischen Eingriffen widersteht oder zumindest zuverlässig signalisiert, dass ein Einbruch stattgefunden hat. Dieser Koprozessor mischt dann mithilfe spezieller Algorithmen die normalen Datenbankabfragen mit künstlich generierten Requests, die das eigentliche Ziel der Abfrage verbergen helfen. Zentrales Problem ist es, den erzeugten Mehraufwand möglichst gering zu halten.[700]

PIR kann besonders für die Nutzung von Hintergrunddatenbanken im UC wichtig werden, um z.B. zu verschleiern, welcher Client einen Service, wie die Informationsbeschaffung zu einem bestimmten Objekt, gerade nutzt. Doch in lokalen UC-Systemen bietet PIR keine Lösung gegen das direkte Sammeln von Informationen über ein Individuum mittels Sensoren.

Ein verschlüsseltes „Outsourcing“ von Clientdaten hingegen ist im UC nur in wenigen Spezialfällen interessant, da die Daten meist erst gar nicht auf dem Client erzeugt und verwaltet werden. Zudem zeigen neuere Forschungsergebnisse bereits in der zugrunde liegenden Theorie solcher Ansätze fundamentale Schwächen, etwa wenn ein zunächst vertrauenswürdiger Datenbankprovider von einem Angreifer übernommen wird.[701]

Die aus Sicht der Sicherheit gebotene Hardwareanforderung von sicheren Koprozessoren in allen betroffenen Servern, der hohe Ressourcenverbrauch und die organisatorische Frage, wie die entsprechenden Schlüssel an jeweils betroffene Clients sicher verteilt und erneuert werden können, sind gewaltige Hindernisse für eine praktische Durchsetzung von PIR für UC.

7.2.4.3.2 Anonymisierung der Kommunikation

Bereits im Internet der Gegenwart zeichnet sich ab, wie schwierig es ist, wirklich Anonymität der Nutzer herzustellen. Die einfache Verschleierung einer IP-Adresse etwa durch NAT oder Proxyserver genügt im Allgemeinen nur gegenüber der Analyse von Traffic und Logfiles auf Serverseite – und auch nur, wenn die eigentliche Anwendung keine eindeutigen Identifikatoren wie Cookies beim Webzugriff oder gar Accountdaten beinhaltet. Gegen Organisationen, die größere Teile des allgemeinen Netzverkehrs überwachen können, ist dies wirkungslos.

[699] Asonov / Freytag, Almost Optimal Private Information Retrieval, PET 2002, S. 209–223; Iliev / Smith, op. cit.

[700] Man kann die Anforderung nach absoluter Unbeobachtbarkeit probabilistisch abschwächen, um effektiveren Zugriffsaufwand zu bewirken, siehe Berthold, Konferenz Wirtschaftsinformatik, 2005, S. 1267–1286.

[701] Evdokimov / Fischmann / Günther, ICDE'06, 2006.

Hier setzen die maßgeblich von David Chaum[702] entwickelten Mixverfahren an, die heutzutage besonders im Onion-Routing[703] mittels TOR[704] oder bei anonymen Proxyservern wie beim AN.ON-System[705] eingesetzt werden.[706]

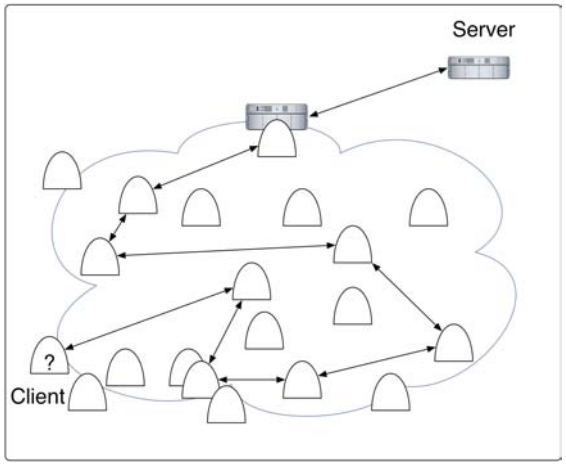


Abbildung 43: Mix-Netze

Die Grundidee besteht darin, in die Kommunikation zwischen Client und Server ein ganzes Netzwerk von Anonymisierungsservern zu schalten, die Nachrichten vieler verschiedener Clients verschlüsselt entgegennehmen. Diese Nachrichten werden untereinander wiederum mehrfach verschlüsselt weitergeleitet und von einer für Dritte nicht mit dem Originalclient in Verbindung zu bringenden Austrittsadresse an den eigentlichen Server gesendet, wobei Antwortpakete den umgekehrten Weg durch dieses Mix-Netz nehmen.

Wie PIR scheint auch die Anonymisierung durch Mixe im UC prinzipbedingt eher für den Zugriff eines Clients auf Hintergrundsysteme geeignet, als für die direkte, lokale Interaktion eines Nutzers mit einer UC-Umgebung. Dies gilt insbesondere, wenn die UC-Umgebung gar nicht auf die aktive Kommunikation mit dem Nutzer angewiesen ist.

Der Grad an Anonymität steigt mit der Anzahl der Teilnehmer und der Dauer, in der Nachrichten auf den einzelnen Mix-Knoten gesammelt werden können, um eine zeitbasierte Traffic-Analyse zu erschweren. Bereits in der Praxis existierende Systeme leiden allerdings auch ohne längeres Zwischenspeichern von Nachrichten unter hohen Latenzzeiten.

Im lokalen UC kommt erschwerend hinzu, dass Anonymität gegenüber einem Betreiber eines UC-Systems in allen verwendeten Grundtechnologien hergestellt werden müsste, was neben dem Netzwerkverkehr auf IP-Ebene oder höher auch eindeutige Adressen auf dem

[702] Chaum, CACM 2(24) February 1981, S. 84–88.

[703] Dingledine / Mathewson / Syverson, TOR – The Second-Generation Onion Router, 2004.

[704] TOR Homepage: http://tor.eff.org/ (31.01.2006).

[705] AN.ON-Homepage (mit Client-Software JAP): http://www.anon-online.de/ (30.03.2006).

[706] Für eine Gegenüberstellung von PIR und Mix-Verfahren siehe Kesdogan / Borning / Schmeink, 2003.

MAC-Layer umfasst. Wenn sich im lokalen System nur wenige oder gar nur einzelne Clients befinden, versagt ein Mix-basierter Ansatz vollkommen.

7.2.4.3.3 Peer-to-Peer-Architekturen (P2P)

Eine Abkehr von zentralen Dienst- und Datenhaltungsstrukturen kann aus der Sicht der informationellen Selbstbestimmung positiv sein, da ein möglicher Profiler Datenspuren nicht nur von wenigen zentralen Orten, sondern von vielen verteilten Instanzen einsammeln müsste, um sie z.B. mittels Data Mining auswerten zu können.[707]

In vielen Anwendungsbereichen könnte man von zentraler Datenhaltung auf Peer-to-Peer-Architekturen[708] (P2P) wechseln. Insbesondere könnte dies neben besserer Lastverteilung auch ein Beobachten des Zugriffs auf bestimmte Daten schwieriger machen, wenn nicht permanent alle P2P-Knoten überwacht werden.[709]

Parallel müssen allerdings Methoden entwickelt werden, Reputation und Vertrauen in solchen Netzwerken zufriedenstellend zu modellieren, implementieren und praktisch handhabbar zu gestalten. Dies wirft insbesondere die Frage der Automatisierbarkeit dieser sozialen Konzepte auf.

Schwierigkeiten bereitet ebenfalls, wie im Abschnitt über Ad-hoc-Netze, die Definition von Identität in solchen Netzen. Ohne zentral verwaltete und überprüfte Identitäten drohen beispielsweise Angriffe mittels „multipler Persönlichkeit“ (Sybil Attack),[710] bei der ein Angreifer große Teile eines P2P-Netzes kontrolliert, indem er viele Identitäten simuliert.

Andererseits widerspricht ein solches zentrales Verfahren dem Grundprinzip der Dezentralisierung und bringt Probleme für die gewünschte Anonymität der Nutzer.

Weitere gravierende Sicherheitsprobleme[711] sind wahrscheinlich, und ohne konkretere Angreifermodelle und entsprechende weitere Sicherheitsmechanismen bewirkt die bloße Verteilung von Daten zunächst keinen Gewinn an Sicherheit. Bei neuen Systemen sollte ein Abwägen von Vor- und Nachteilen der Wahl einer bestimmten P2P-Architektur für die informationelle Selbstbestimmung und Informationssicherheit der Nutzer bereits früh in der Designphase erfolgen.

7.2.5 Zusammenfassung

Informationssicherheit im UC ist ein äußerst komplexes und schwieriges Problem. Insoweit

---

[707] Einen Vergleich von Mix- und P2P-Systemen bzgl. verschiedener Angreifermodelle bieten Böhme et al., 2005.

[708] Überblick: Steinmetz / Wehrle (Hrsg.), 2005; Birman, Reliable Distributed Systems, 2005, S. 531ff.

[709] Ein datenschutzfreundliches P2P-System, das auch Ideen aus Mix-Netzen verwendet, ist Freenet: Clarke et al., IEEE Internet Computing, 2003, S. 40–49; Projekt-Homepage: http://freenetproject.org/ (16.03.2006).

[710] Douceur, The Sybil Attack, 2002.

[711] Z.B. Datenintegrität.

als UC und das Internet der Dinge zu direkten Nachfahren des klassischen Internets werden oder sich in den gekoppelten Hintergrundsystemen direkt darauf stützen, erbt es die klassischen Probleme mangelnder IT-Sicherheit, allerdings verbunden mit zu schützenden Datenmassen in ungekannter Quantität und Qualität.

Aber auch in den neuen lokalen Technologien wie RFID zeichnet sich eine Vielzahl von Sicherheitsproblemen ab. Zunächst gibt es bei der Marktfähigkeit der einzelnen im UC benutzten Geräte und Chips das Optimierungsproblem zwischen den Parametern Leistungsfähigkeit, Größe, Energieverbrauch und Preis. Ihre Leistungsfähigkeit wird oft, wie z.B. bei einfachen RFID-Tags und Sensorknoten, zum Erreichen eines günstigen Stückpreises so minimiert, dass die Hauptfunktion des jeweiligen Geräts in einem idealen Normalbetrieb erfüllt werden kann. Doch die Realisierung von Informationssicherheit im UC benötigt Bausteine wie symmetrische oder asymmetrische Verschlüsselung, Zufallszahlen und kryptographische Hashfunktionen. Trotz erfreulicher Fortschritte auf diesem Gebiet ist beispielsweise gerade bei den für den Massenmarkt vorgesehenen Class-1-RFID-Tags diese Voraussetzung nicht erfüllt.

Diese Bausteine werden in kryptographischen Protokollen verwendet, die sorgfältig auf ihre Korrektheit geprüft werden müssen, bevor Aussagen zu ihrer Sicherheit getroffen werden können. Dies ist für neue Protokolle, die an die Gegebenheiten des UC angepasst werden, ein offenes theoretisches Forschungsfeld.

Kryptographie verwendet Schlüssel, die in der Praxis auch sicher verteilt und regelmäßig geändert sowie im Kompromittierungsfall zurückgerufen werden müssen. Dies wirft technische und organisatorische Fragen zur Skalierbarkeit und Sicherheit dieses Schlüsselmanagements auf, nahezu ein Teufelskreis gerade angesichts der offenen und teilweise spontan gebildeten UC-Netze. Reputations- und Web-of-Trust-Ansätze können dieses fundamentale Problem nur lindern, nicht lösen.

Auch sollte jede Lösung für Informationssicherheit und informationelle Selbstbestimmung im UC leicht zu bedienen sein, sonst drohen durch die fehlerhafte Bedienung überforderter Nutzer viel größere Sicherheitslücken als nur durch Mängel in der zugrunde liegenden Kryptographie.

Wenn sich ferner die Fehler in der Softwareentwicklung, die im heutigen Internet Betriebssysteme, Client- und Serversoftware sowie inzwischen PDAs, Mobiltelefone und sogar Autos heimsuchen, in das UC fortsetzen, so droht die positive Vision des UC zu einem „ubiquitären Alptraum“ für die Betreiber und Nutzer zu werden.

7.3 Selbstbestimmung im Ubiquitous Computing

Wichtig für Selbstbestimmung in einer Umwelt von UC-Systemen ist, neben ihrer Sicherheit, besonders der Grad an Kontrolle, die ein Individuum über sie ausüben kann. Wichtige Teilaspekte sind neben Offenheit die Kontrolle über die genutzten Geräte und die eigenen Daten im UC, sowie, als psychologischer Faktor, die Verfügungsgewalt über die eigene Aufmerk-

samkeit als begrenzte Ressource.[712]

Wir untersuchen im Folgenden einige zentrale technische und organisatorische Lösungen, die geeignet erscheinen, die Kontrolle durch das Individuum im UC zu fördern.

7.3.1 Offenheit im Ubiquitous Computing

Verschiedene Facetten von Offenheit[713] können die Entwicklung des UC und die Selbstbestimmung des Individuums im UC fördern. Offene Standards für UC-Technologie, d.h. insbesondere auch Standards, die einfach zugänglich – d.h. möglichst unentgeltlich und ohne Lizenzgebühren – von jedermann genutzt werden können, erhöhen neben der Interoperabilität von UC-Systemen auch ihre Transparenz. Diese stellt eine notwendige Bedingung für die Kontrolle durch den Nutzer und seine Selbstbestimmung dar.

Hier sind besonders offene Datenformate, Schnittstellen und Architekturen zu nennen. Beispielsweise ist trotz der in Kap. 7.2.4.2.1 zur Sicherheit diskutierten Schwächen als ein positiver Aspekt im Design des EPC-Netzwerks zu nennen, dass es den Versuch unternimmt, auf bereits etablierte und standardisierte Protokolle und Schnittstellen zurückzugreifen (auch wenn die Wahl des unsicheren DNS unglücklich erscheint). Theoretisch stünde einer Anbindung von Open Source-Lösungen an das EPC-Netzwerk zumindest aus technischer Sicht nichts entgegen – sofern die Nutzung des eigentlichen EPC lizenzrechtlich frei bleibt.

Die Entwicklung und der Einsatz von Open Source-Software im UC erscheint aus Sicht der Offenheit ideal, wenn er sich mit den Geschäftsmodellen der Hersteller und Betreiber verbinden lässt. Mit Open Source wäre, zumindest potentiell, Transparenz und Modifizierbarkeit besonders auch der lokal eingesetzten UC-Technologie gewährleistet.[714]

Hinzutreten muss Transparenz von Datenfluss, -haltung und -auswertung, was nicht nur durch die Auswahl einer Technologie erreicht werden kann, sondern durch organisatorische und gesetzliche Rahmenbedingungen unterstützt werden muss. Einige solcher Ansätze behandeln wir in Kap. 7.3.3.

Schließlich gehört zur Selbstbestimmung im UC auch die Offenheit im Zugang zu seinen Systemen und dem damit verbundenen Nutzen. Einerseits müssen UC-Systeme beispielsweise auf die Bedürfnisse gesellschaftlicher Minderheiten wie z.B. Behinderter eingehen können, was nicht an mangelnder Übereinstimmung eines Kontextes mit einer wie auch immer definierten „Norm“ scheitern darf. Andererseits bietet das enorme Volumen an gesam-

---

[712] Davenport / Beck, 2001.

[713] Zu differenzieren vom rein technischen Begriff des „offenen Systems“, wie im Kap. 7.2.2.1 charakterisiert.

[714] Ohne an dieser Stelle ausführlich auf die Auswirkungen des Einsatzes von Open Source auf die IT-Sicherheit eingehen zu können (siehe z.B. Hansen / Köhntopp / Pfitzmann, 2002), sind wir von der positiven Wirkung überzeugt, jedenfalls soweit IT-Sicherheit als technisches Phänomen charakterisierbar ist und nicht realiter als hauptsächlich organisatorisches. Ein Paradebeispiel für hohe Sicherheit bei Open Source ist das OpenBSD-Projekt, http://www.openbsd.org/ (06.03.2006).

melten Daten die Gelegenheit zu noch ungeahnter Personalisierung, und, als Schattenseite, Diskriminierung der Nutzer. Besonders für den letzten Aspekt zeichnen sich leider noch nicht einmal Ansätze von technischen oder organisatorischen Lösungen ab.

7.3.2 Kontrolle über Hard- und Software

Eine wichtige Anforderung der Selbstbestimmung ist, dass ein Nutzer stets, wenn er will, eine möglichst vollständige Kontrolle über die mit ihm interagierenden Geräte in seiner Umgebung erhalten kann, soweit dies nicht mit den Interessen anderer Nutzer kollidiert. So sollte niemand anderer als der Nutzer auf seinen eigenen Geräten gespeicherte Daten auslesen oder manipulieren, Software und Konfiguration verändern oder Nutzungsbeschränkungen verhängen dürfen, insbesondere auch nicht Firmen zu Zwecken eines Digital Rights Managements (DRM) im UC.[715]

Insbesondere gilt diese Forderung natürlich für Geräte, die sich im Besitz des Nutzers befinden, so unter anderem die RFID-Tags an seiner Kleidung, Sensoren im PAN und andere Geräte. Aber auch in einem Fahrzeug oder Smart Home sollte die Grenze der technischen Kontrolle mindestens mit der Eigentumsgrenze übereinstimmen, wenn nicht, zumindest temporär, sogar darüber hinausreichen. Die Kontrolle über etwaige „Trusted Computing"-Systeme muss beim Nutzer (oder bei Instanzen seines Vertrauens) liegen, und nicht bei externen Parteien, die die UC-Umgebung sonst „fremdbestimmen" könnten.

Diese Forderung entspricht der starken Bindung zwischen „Mother" und „Duckling" im weiter oben (in Kap. 7.2.3.1) diskutierten „Resurrecting Duckling"-Modell. Bei einer technischen Umsetzung könnte zum Beispiel ein zentrales „Master Device" aus dem Besitz des Nutzers stellvertretend für ihn als „Mother" eine ganze Gruppe von „Ducklings" kontrollieren. Natürlich müssen zur effektiven Ausübung von Kontrolle durch den Menschen geeignete Interfaces geschaffen werden.

Skepsis erscheint angebracht, ob eine solche Anforderung sich auch sicher umsetzen lässt. Doch da auch ein von außen gesteuertes UC nicht sicher ist, sondern neben einem vorgesehenen externen Kontrolleur potentiell ebenfalls auch einen erfolgreichen Angreifer zu Gast haben kann, muss hier eine Abwägung beim Design der konkreten Systeme erfolgen.

7.3.3 Kontrolle über Daten

Zur Selbstbestimmung des Nutzers im UC gehört auch die Kontrolle über möglichst viele der über ihn erfassten Daten (vgl. Kap. 7.2.3.2.8). Ein wichtiger Spezialfall ist das aus der Informationssicherheit bekannte Problem der Zugriffskontrolle auf Nutzerdaten (vgl.

[715] Die ökonomischen Motive für ein DRM auf Basis von Rootkits wie in einigen aktuellen Kopierschutzsystemen dürften auch im UC weiter bestehen; solche Systeme im UC würden mit hoher Wahrscheinlichkeit ähnliche negative Effekte für die Sicherheit der Systeme und das Vertrauen der Nutzer hinterlassen. Vgl. Russinovich, Mark: http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html (02.02.2006); Hansen, DuD 30 (2006), 2, S. 95-97.

Kap. 7.2.3.2.5 für den Spezialfall RFID). Im folgenden Abschnitt werden einige der dort besprochenen Ansätze auf ihre Machbarkeit im allgemeinen UC untersucht.

Jede allein technisch umgesetzte Lösung zur direkten Kontrolle von Daten wird allerdings spätestens dann scheitern, wenn die Datenerhebung gar nicht im Rahmen eines technischen Kommunikationsvorgangs (etwa via RFID, WLAN, Bluetooth) erfolgt, sondern von Sensoren (analog zu einer Videoüberwachung) passiv und unauffällig durchgeführt wird, ohne dass ein technisches Schutzsystem es verhindern könnte.[716] In solchen Fällen ist zudem nicht sichergestellt, dass die Betroffenen überhaupt bemerken, dass Daten über sie erfasst und verarbeitet werden, so dass ggf. eine Benachrichtigungspflicht erforderlich ist. Da im UC starke Anreize für die Betreiber bestehen, die qualitativ hochwertigen Daten über Nutzer zu sammeln,[717] gibt es keine technische Lösungen ohne eine starke Flankierung durch klare rechtliche Maßnahmen, die wiederum auch wirklich durchgesetzt werden müssen.

7.3.3.1 P3P und PawS (Privacy Awareness System)

Der Vorschlag des Projekts „Platform for Privacy Preferences“ (P3P)[718] für das Web ist es, eine XML-basierte, maschinenlesbare Datenschutzerklärung[719] (Policy) zu erstellen. Damit kann ein automatisierter Abgleich zwischen den Datenschutzeinstellungen des Nutzers im Web-Browser und der Datenschutzerklärung des Website-Betreibers erfolgen.

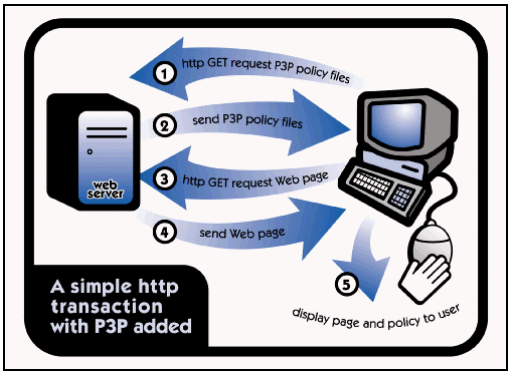


Abbildung 44: Eine P3P-Transaktion (Quelle: W3C[720])

Diese Idee ist von P3P-Designern auf UC-Umgebungen übertragen worden.[721] Im sogenann-

[716] Als fundamentales Problem gesehen auch in Ranganathan, 2002, ohne Hinweise darauf, wie die dort geforderten Änderungen der allgemeinen Rechner-, Computer- und Netzwerkinfrastrukturen sicher und auch nur ansatzweise überprüfbar umgesetzt werden könnten.

[717] Für RFID siehe Bauer / Fabian / Fischmann / Gürses, 2006; Albrecht / McIntyre, 2005; zur generellen Problematik z.B. Garfinkel, 2000.

[718] P3P Projekt: http://www.w3.org/P3P/ (01.02.2006).

[719] Siehe W3C, P3P1.1, 2005.

[720] P3P Public Overview: http://www.w3.org/P3P/brochure.html (01.02.2006).

[721] Langheinrich, A Privacy Awareness System for Ubiquitous Computing Environments, 2002; Langheinrich, Dissertation, ETH Zürich, 2005. Für eine verwandte Lösung zu RFID siehe oben den Kap. 7.2.3.2.8.2.

ten „Privacy Awareness System“ (PawS) gibt es folgende Hauptkomponenten: Privacy-Assistent (PA), Privacy-Beacons (Leuchtfeuer im übertragenen Sinn), Privacy Proxies und „Privacy-aware“ Datenbanken. Der PA ist ein kleines Gerät im mobilen Besitz des Nutzers, das die von den in jeder UC-Umgebung vorhandenen Beacons ausgesendete Privacy Policy empfängt. Diese Policy kann z.B. den Betreiber des UC-Systems kennzeichnen und enthält in maschinenlesbarer Form den Verwendungszweck der in diesem System – z.B. mithilfe von Sensoren – gesammelten Daten. Die Aussendung der Policy oder eines ihr entsprechenden Identifikators kann implizit in lokale Service Discovery-Protokolle integriert sein, oder explizit – z.B. bei Videoüberwachung – auf einem anderen Kommunikationsweg vermittelt werden.

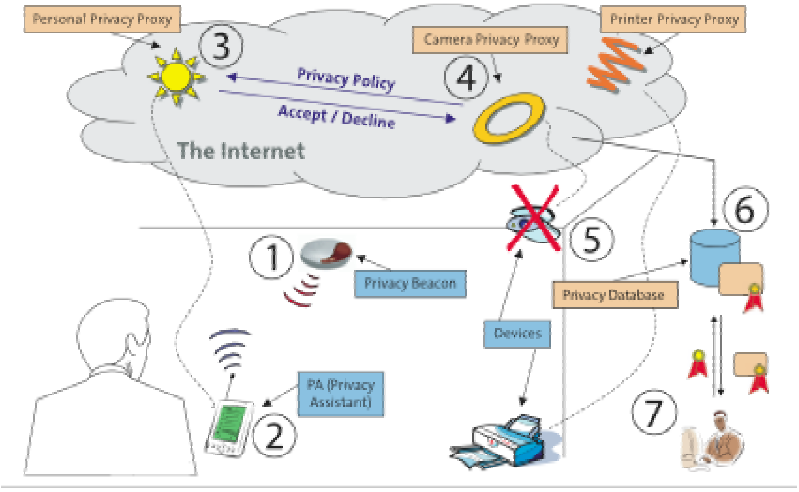


Abbildung 45: PawS-Architektur (Langheinrich, 2005)

Verbunden mit dieser Interaktion lokaler Systeme ist eine Architektur internetbasierter Hintergrundsysteme. Der „Personal Privacy Proxy“ ist ein System, das im Auftrag und unter der Kontrolle des Nutzers stellvertretend für ihn mit den Privacy Proxies des UC-Systems interagiert, z.B. eine ausführliche Policy herunterladen oder zur lokalen Interaktion nötige Daten des Nutzers dem System – unter Vorbehalt der Akzeptanz der verkündeten Datenschutzerklärung – bereitstellen, ändern oder wieder löschen kann. Diese Proxies sollen jederzeit im Internet erreichbar sein.

Die „privacy-bewussten“ Datenbanken speichern persönliche Nutzerdaten nur als eine Einheit mit der zugehörigen Policy, wachen über ihre Einhaltung und ermöglichen Audits.

Die Verknüpfung der lokalen Geräteinteraktion mit Hintergrundsystemen im Internet, die Daten des Nutzers und der UC-Umgebung verwalten, führt zu erhöhtem Aufwand für die IT-Sicherheit. Der Einsatz von P3P muss mit rechtlichen und organisatorischen Maßnahmen flankiert werden, da er keine technisch gesicherte Durchsetzung der individuellen Privacy-

Präferenzen beinhaltet.[722] Zwar wird unter dem Begriff „Privacy Management Languages“ an Erweiterungen von P3P und verwandten Ansätzen gearbeitet, die die vorgegebenen Policies auch unmittelbar technisch umsetzen. Diese Systeme setzen allerdings die Kooperation der Betreiber voraus und funktionieren nur in dem von ihnen kontrollierten Bereich. Auch sie können für einen Einsatz innerhalb einer offenen Umgebung mit der Möglichkeit von absichtlichem Missbrauch personenbezogener Daten keine technische fehlerfreie Umsetzung von Privacy Policies garantieren. Es erscheint nahezu unmöglich, die Einhaltung entsprechender Policies im UC in hinreichendem Maßstab zu überprüfen.

7.3.3.2 Trusted Computing und DRM für Privacy

Die Forderung, dem Nutzer wirkliche Kontrolle über seine Daten einzuräumen und nicht nur auf Datenschutzerklärungen zu vertrauen, führt zu der Idee, zu diesem Zweck eine Form von Digital Rights Management (DRM) und Trusted Computing (TC) in UC-Systemen zu verwenden.[723] Dabei könnte TC als technische Grundlage dafür dienen, Privacy-DRM auch sicher auf Geräten durchsetzen zu können, die sich nicht im Besitz oder außerhalb der physischen Reichweite des UC-Nutzers befinden.[724]

Privacy-DRM ist eine bestechende Idee, hat aber diverse praktische Hindernisse. Ein zentrales Problem ist, wer den zusätzlichen organisatorischen und technischen Aufwand bezahlen wird – Firmen werden diese Mehrkosten nicht freiwillig übernehmen. Subtiler noch ist der psychologische Faktor: Die Kontrolle über eigene Server auch nur teilweise an Außenstehende abzugeben, dürfte IT-Verantwortlichen nicht leicht fallen.

Offen ist auch die Frage, ob so ein Verfahren ohne eine Form von globaler PKI machbar ist und ob es wegen des notwendigen Management-Overheads gar nicht erst in Gang kommt. Gegen wirklich böswillige Datensammlung, die Zugriff auf zur Verwendung freigegebene Daten hat und diese mittels unkontrollierter Hardware kopiert, kann Privacy-DRM nicht schützen, ebenso wenig gegen unauffällige und passive Datensammlung durch Sensoren.

7.3.4 Kontrolle über Aufmerksamkeit

Als fundamentale und äußerst knappe Ressource im UC kann die menschliche Aufmerksamkeit betrachtet werden. Wie mit ihr in UC-Systemen umgegangen wird, die eine Vielzahl von neuen Schnittstellen zwischen Mensch und intelligenter Umgebung bereitstellen werden,

---

[722] Zur Problematik von P3P und ähnlichen Verfahren im UC siehe auch Gow, ITU, 2005, S.10f. Diskussion zu Problemen von und durch P3P: Coyle, Karen, 1999: http://www.kcoyle.net/p3p.html ; EPIC, 2000: http://www.epic.org/reports/prettypoorprivacy.html ; Clarke, Roger: http://www.anu.edu.au/people/Roger.Clarke/DV/P3PRev.html (13.03.2006).

[723] Für RFID z.B. vgl. Molnar / Soppera / Wagner, Privacy for RFID Through Trusted Computing, 2005.

[724] Hansen, Ein zweischneidiges Schwert – Über die Auswirkungen von Trusted Computing auf die Privatsphäre, 2004, sowie Hansen / Möller, Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung, 2005.

könnte großen Einfluss auf die Akzeptanz solcher Systeme im Alltag besitzen.

Zwei gegensätzliche Grundkonzepte lassen sich identifizieren, die wie immer in der Praxis des UC zahlreiche Mischformen aufweisen werden:

- „Push"-basierte Interaktion, wo die „intelligente Umgebung" auf den Menschen eindringt und Aufmerksamkeit einfordert, und
- „Pull", wo der Mensch zuerst auf die Umgebung zugeht, und eine Interaktion, die seine Aufmerksamkeit erfordert, selbst initiiert.

Im Anschluss folgen einige heutige Beispiele für diese Interaktionsformen, die allerdings nur erste Antagonisten bzw. Vorläufer eines im Hintergrund verschwindenden UC im Sinne des „Calm Computing" darstellen.

7.3.4.1 Push: SPAM im Ubiquitous Computing

Ein UC-System, das hauptsächlich mittels „Push" funktioniert, könnte sehr schnell als Verbreiter von Spam[725] aufgefasst und blockiert werden – so denn eine Blockade überhaupt möglich ist, ohne die Nutzung anderer Funktionen oder Dienste in Mitleidenschaft zu ziehen.

Ein Beispiel aus der Gegenwart, wie eine Push-basierte UC-Umgebung funktioniert, bietet das Versenden von Werbung mittels Bluetooth als Vorstufe zur interaktiven Plakatwand[726].

„Eine völlig neue Form der Kundenansprache wird möglich: Weil der Konsument den Download ja genehmigen muss, kann der Werber sich seiner gesteigerten Aufmerksamkeit sicher sein - ganz anders als bei Plakatwänden."[727]

Dieser Form von Spam kann man sich nur entziehen, indem man die Bluetooth-Funktionalität des Handy deaktiviert – was zwar aus anderen Gründen, nämlich der IT-Sicherheit, zur Zeit ebenfalls ratsam ist, aber doch die Kollateraleffekte von Push-Architekturen hervorragend demonstriert.

7.3.4.2 Beispiele für Pull-Architekturen

Eine positive Alternative in einem ähnlichen Anwendungskontext wie die interaktive Plakatwand bietet das freie Projekt Semapedia.[728] Hier kann man eine URL in einen optischen Code übersetzen lassen, den man dann an einem physischen Objekt oder einem Gebäude anbringt.

[725] Cf. Wikipedia, s.v. „Spam".

[726] Bluespot-Marketingsystem der Firma Wall, http://www.wall.de/de/city_marketing/concept/bluespot/index.asp / www.bluespot.de (03.02.2006).

[727] Spiegel online, 05.01.2006: http://www.spiegel.de/netzwelt/technologie/0,1518,393376,00.html (03.02.2006).

[728] Projekt Semapedia, http://www.semapedia.org/ (03.02.2006).

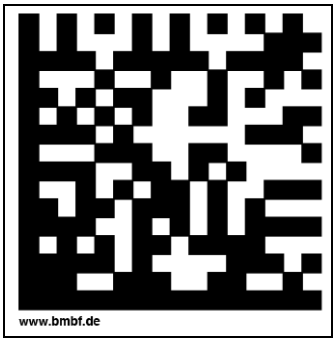


Abbildung 46: Optischer Semapedia-Tag mit kodierter URL

Der Nutzer kann selbst entscheiden, ob er mehr Informationen zu seiner physischen Umgebung einholen möchte und gewissermaßen in Kontakt mit der „Embedded Virtuality" treten möchte. Mithilfe einer speziellen Software auf einem Photohandy kann er den optischen Tag photographieren, wieder in eine URL übersetzen und somit einen Web-Artikel über das jeweilige Gebäude oder den Gegenstand aufrufen – dieselbe Anwendung wie bei obigem Bluetooth-System, allerdings hier mittels einer Pull-Architektur gelöst.

Ein anderes Beispiel für eine Interaktionsarchitektur im UC, bei der die Nutzer die Initiative besitzen und auf die UC-Umgebung zugehen, ist Elope.[729]

Grundidee ist, mit Tags versehene Objekte in einem interaktiven Raum und mobile Geräte des Nutzers mithilfe einer Middleware (namens Elope) zu verbinden. So kann z.B. ein kleines, mobiles Gerät die weitaus bessere Qualität der in einem interaktiven Raum befindlichen Interfaces (Bildschirme, Surround-Soundsysteme) nutzen, ohne dass aufwendige Konfigurationsarbeit notwendig wäre.[730] Verschiedene Konfigurations- und Nutzungsoptionen sind in RFID-Tags auf speziellen Objekten hinterlegt, wie zum Beispiel auf der Fernsteuerung eines Beamers.

Der Nutzer zeigt mit dem Handy einfach auf das Objekt (Pull). Das Handy wiederum liest mithilfe eines integrierten RFID-Readers den Tag aus und verwendet die gespeicherte Bluetooth-Konfiguration zur Kontaktaufnahme mit dem Projektor, der dann im Handy gespeicherte Bilder oder Filme anzeigt.

Ein wichtiges Designziel des Elope-Projekts ist die möglichst konfigurationsfreie Nutzung der UC-Umgebung; gleichzeitig wird das Prinzip umgesetzt, dass der Nutzer die Interaktion mit der Umgebung – auch haptisch, mit dem symbolischen Zeigen auf das Interaktionsziel – initiiert. Natürlich kann es UC-Anwendungen geben, in denen Interaktion anders initiiert werden muss, dennoch bleibt dieser Ansatz paradigmatisch. Ausgeblendet sind in dieser Kernidee die Anforderungen der Nutzer und Betreiber an Sicherheit und Datenschutz. Spätestens in diesem Projektstadium müssen sich Designer intensiv mit entsprechenden Fragen ausei-

[729] Pering et al., CACM 48 (9), September 2005, S. 53–59.

[730] Gewissermaßen eine klassische „Uranwendung" des UC, vgl. Weiser, Scientific American 265, 1991, S. 66–75; Weiser, CACM 36 (7), 1993, S. 75–84.

nandersetzen.[731] Ohne Sicherheitsmechanismen wären z.B. private Daten auf dem Mobilgerät ungeschützt, oder die Architektur kann trotz des ursprünglichen Designs leicht für Spam (Push) missbraucht werden.

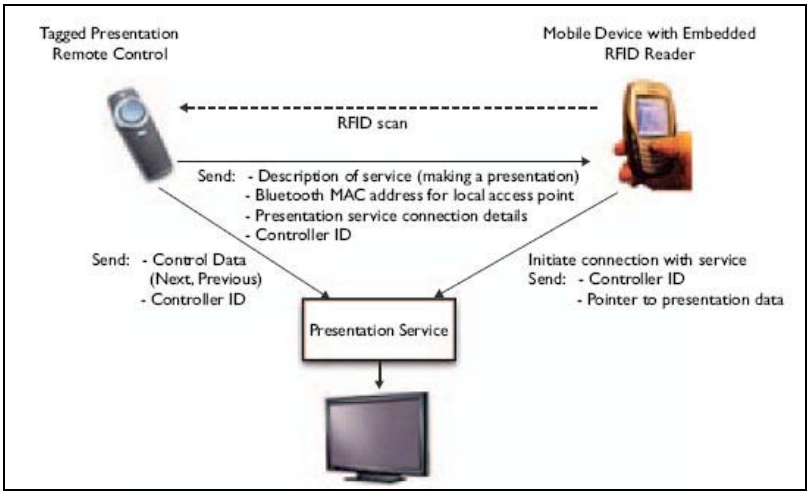


Abbildung 47: Elope Architektur (Pering, 2005)

7.3.4.3 HCI: Delegation vs. Detailkontrolle

Das oben diskutierte Elope-Projekt deutet – neben der vom Nutzer initiierten Interaktion - bereits ein weiteres wichtiges Designkriterium für UC-Systeme an: Die Benutzung muss einfach und möglichst ohne viel Konfigurationsaufwand möglich sein – nur so kann einerseits die Vision des ruhigen, des „Calm Computing“[732] umgesetzt und Akzeptanz erreicht werden. Dazu ist Delegation von Aufgaben an die intelligente Umgebung nötig, etwa an Softwareagenten.

In gewissem Sinne bildet die Forderung nach Detailkontrolle, d.h. objektiver Kontrolle des Nutzers über die UC-Umgebung, dazu einen Antagonismus, denn nur durch detaillierte Informationen können technische Prozesse wirklich erfasst und ihre Auswirkungen abgeschätzt werden, so dass ein Individuum durch seine Entscheidungen Einfluss darauf nehmen kann.

Somit ist eine wichtige Anforderung, dass ein Nutzer jederzeit und nach Wunsch komfortabel auf möglichst viele der ihn betreffenden automatischen Prozesse direkt durch manuelle Konfigurationsmöglichkeiten einwirken und Vorgänge rückgängig machen kann. Sofern er dem initial zustimmt (opt-in statt opt-out), können anschließend Automatismen im Sinne des „Calm Computing“ ohne sein Einwirken ablaufen, so zum Beispiel mithilfe von Softwareagenten.[733] Bedingung dafür ist allerdings, dass dem Nutzer rechtzeitig bewusst wird, in welchen

[731] Wir verzichten an dieser Stelle auf eine detaillierte Sicherheitsanalyse.

[732] Weiser / Brown, The Coming Age of Calm Technology, 1996.

[733] Diese müssen dem Nutzer gegenüber allerdings wirklich „loyal“ sein, womit sich auch hier die fundamentale Bedeutung der Informationssicherheit im UC zeigt.

Fällen er möglicherweise Einfluss nehmen oder Vorgänge rückgängig machen möchte.

Natürlich wird jeweils die praktische Umsetzung dieser abstrakten Anforderungen Kompromisse eingehen müssen, die beiden Grundziele, Schonung der Aufmerksamkeit bei maximaler individueller Kontrollmöglichkeit sollten einen Leitfaden beim Design von UC-Systemen bilden, insbesondere beim Design der Schnittstellen und Interaktion zwischen Mensch und Maschine (Human Computer Interaction, HCI).

Abzuwarten bleibt, ob und inwieweit kontextsensitive Systeme diesen Zwiespalt lösen können.

7.3.5 Identitätsmanagement im Ubiquitous Computing

Eng verbunden mit dem Problem der Selbstbestimmung des Individuums im UC ist die Frage, was Identitäten im UC bedeuten, und wie sie zufriedenstellend technisch modelliert und im Alltag so gehandhabt werden können, dass die informationelle Selbstbestimmung bewahrt wird. Bereits in Kap. 7.2.3.3 zur Sicherheit von Ad-hoc-Netzen wurden entsprechende Schwierigkeiten offenbar.

Der Begriff „Identitätsmanagement“ wird von unterschiedlichen Seiten unterschiedlich verstanden und interpretiert. Betrachtet man die Art der Verwaltung und die verwalteten Daten, so erhält man drei Typen von Identitätsmanagementsystemen (IMS):

- Typ 1: IMS zur zentralen Verwaltung von Benutzern und ihren Zugriffsrechten (Authentifizierung, Autorisierung, Accounting) durch Organisationen, vorwiegend durch Einsatz von Verzeichnisdiensten (z.B. LDAP).
- Typ 2: IMS zum Profiling von Nutzerdaten (z.B. Scoring-Verfahren) durch Organisationen.
- Typ 3: IMS zur nutzerkontrollierten kontextabhängigen Verwaltung von Rollen und Pseudonymen. [734]

In vielen Fällen handelt es sich in der Praxis um Mischformen, die allerdings häufig einen Schwerpunkt in einem der genannten Typen aufweisen. Diese Kategorien werden zunächst im Anschluss näher erläutert, danach wird die Anwendbarkeit von IMS für UC diskutiert.

7.3.5.1 IMS vom Typ 1

IMS vom Typ 1 kommen dort zum Einsatz, wo innerhalb eines kontrollierten Umfeldes Berechtigungen zentral verwaltet werden. Neben den bereits genannten Verzeichnisdiensten werden auch bekannte Konzepte wie Liberty Alliance[735] oder Microsoft Passport[736] (soge-

nannte Single Sign-On-Dienste) primär diesem Typ zugeordnet, soweit die Datenverwaltung nicht unmittelbar unter Kontrolle des Nutzers steht. Auch einige Digital Rights Management-Systeme entsprechen diesem Prinzip.

Charakteristisch für IMS vom Typ 1 ist, dass die Nutzer selbst ihre Berechtigungen nicht ändern können, sondern das System dazu dient, zentral festgelegte Berechtigungen organisationsweit durchzusetzen.

7.3.5.2 IMS vom Typ 2

IMS vom Typ 2 kommen zum Einsatz, wenn aus anfallenden Daten Aussagen über Nutzer herauskristallisiert werden sollen, z.B. für Marketingzwecke, um Kunden bestimmten Verhaltensgruppen zuzuordnen und daraus resultierend deren zukünftiges Kaufverhalten vorauszusagen und ggf. zu beeinflussen (Profiling).[737] Ebenfalls Typ 2 entsprechen Systeme, die das potentielle Ausfallrisiko eines Interessenten für einen Bankkredit benennen sollen (z.B. Scoring-Systeme für Kreditwürdigkeit).

Im UC wird eine Umgebung, die versucht, auf Basis vorheriger Entscheidungen oder Verhaltensweisen eines Nutzers sich automatisiert und ohne dessen Mitwirken auf diesen einzustellen, sich eines Typ 2-IMS bedienen. Wie die Ergebnisse der Befragung in Kapitel 5 verdeutlichen, ist bei Typ 2-gestützten UC-Umgebungen eher von einer Ablehnung durch die Benutzer auszugehen, die sich in ihrer Privatsphäre bedroht fühlen und die aufgrund von Profiling-Ergebnissen ausgeführten Aktionen als Kontrollverlust empfinden.

---

[734] Bauer / Meints / Hansen: Structured Overview on Prototypes and Concepts of Identity Management Systems, 2005.

[735] Siehe z.B. Liberty Alliance, 2003.

[736] Ein Nachfolgesystem desselben Herstellers ist InfoCard, das viele Aspekte von Typ 3-IMS aufweist, vgl. Microsoft, 2005.

[737] Hildebrandt / Backhouse: Descriptive Analysis and Inventory of Profiling Practices, 2005.

7.3.5.3 IMS vom Typ 3

IMS vom Typ 3 sind nutzerzentriert und dezentral organisiert. Die Nutzer selbst verwalten die Daten über sich und können Vorgaben treffen, wann diese wem gegenüber wie preisgegeben werden. In Form von z.B. Passwort-Managern findet man bereits heutzutage erste Teillösungen.

Das in vielen UC-Szenarien anzutreffende technische Hilfsmittel eines persönlichen digitalen Assistenten, der die Steuerung der UC-Umgebung anhand vom Nutzer gewählter Präferenzen übernimmt, statt sie der Umgebung selbst zu überlassen, und darüber hinaus dem Nutzer das Wissen über die Verarbeitung der ihn betreffenden Daten ermöglicht, stellt eine Inkarnation eines IMS vom Typ 3 dar. Derartige Konzepte sind die einzigen IMS, die dem Nutzer selbst eine Kontrolle im UC überlassen. Es wird daher erwartet, dass Typ 3-Systeme verglichen mit den anderen Typen die größte Nutzerakzeptanz erreichen werden, denn Datenschutzgesichtspunkte sind oft eine treibende Kraft hinter der Entwicklung von Typ 3-IMS und relevantes Alleinstellungsmerkmal am Markt.[738]

7.3.5.4 IMS in UC-Umgebungen

Im UC ist davon auszugehen, dass Nutzer vor allem auf hybride Systeme treffen werden, die sich nicht eindeutig einem Typ zuordnen lassen.

Wenn z.B. im Arbeitsumfeld der Arbeitgeber Zutrittsberechtigungen zu Räumen für bestimmte Personen oder Gruppen festlegt, legt dies die Kategorisierung als IMS vom Typ 1 nahe. Die Einordnung ist jedoch davon abhängig, wie in diesem Fall die Authentisierung durchgeführt wird. Sofern anhand eines z.B. RFID-basierten Betriebsausweises die Zuordnung erfolgt, liegt ein Typ 1-IMS nahe, während bei Nutzung eines persönlichen digitalen Assistenten ein Typ 3 anzunehmen ist.

Im Sinne eines Lösungsansatzes für Gefährdungen der Privatsphäre sind Systeme vom Typ 3 zu bevorzugen. Es ist daher wenig verwunderlich, dass die Europäische Union gerade in diesem Bereich Projekte zu Forschung und Entwicklung fördert.[739] Insbesondere im Projekt PRIME soll ein nutzerkontrolliertes IMS nach europäischem Recht zur täglichen Nutzung durch die Informationsgesellschaft entwickelt und implementiert werden. Dafür wird eine datenschutzfördernde Technikplattform vorgeschlagen, die die Handelnden in der Wahrnehmung ihrer Rollen und gegenseitigen Verantwortungen unterstützt. Dafür wird eine große Akzeptanz zum Vorteil aller erwartet.[740]

Für Nutzer verunsichernd dürfte sein, dass sie sich der Annahme, ein nutzerzentriertes Typ 3-IMS vor sich zu haben, nicht sicher sein können, da ein Typ 2-IMS auch unbemerkt im

---

[738] Bauer / Meints / Hansen: Structured Overview on Prototypes and Concepts of Identity Management Systems, 2005.

[739] Z.B. die Projekte PRIME – Privacy and Identity Management for Europe, http://www.prime-project.eu.org/ und FIDIS – Future of Identity in the Information Society, http://www.fidis.net/ (13.03.2006).

[740] Hansen / Krasemann: PRIME White Paper, 2005.

Hintergrund mitlaufen kann. Während ein Typ 3-IMS den Nutzern ermöglicht, die Verarbeitung ihrer personenbezogenen Daten kontrollierend zu beeinflussen, haben sie dadurch keine Sicherheit, dass nicht parallel noch eine weitere, nicht beeinflussbare Verarbeitung stattfindet. Eine technisch effektive Lösung zur Verhinderung nicht-selbstkontrollierter Verarbeitung personenbezogener Daten kann damit daher nicht gewährleistet werden. Organisatorische (z.B. legislative) Maßnahmen, die dies auffangen sollen, können einen Missbrauch der anfallenden Daten zwar sanktionieren, jedoch nicht verhindern. Aufgrund der immensen Menge personenbezogener Daten, die in UC-Szenarien ausgewertet und somit anfallen werden, ist daher auch von einem entsprechend hohen Missbrauch auszugehen.

7.4 Zusammenfassung und Ausblick

„Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. As organizations in both the private and the public sectors routinely exchange such information, individuals have no way of knowing if the information is inaccurate, obsolete, or otherwise inappropriate. The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a "chilling effect," causing people to alter their observable activities. As computerization becomes more pervasive, the potential for these problems will grow dramatically." (Chaum, 1985).

Die Entwicklung von technischen und organisatorischen Lösungen für die Selbstbestimmung des Individuums im Ubiquitous Computing steht auch 20 Jahre nach Chaums Bemerkung noch ganz am Anfang.

Fundamental dafür ist zunächst, wie IT-Sicherheit im UC eingefordert, geplant und umgesetzt wird, aber auch, welche Grenzen sie findet. Ubiquitous Computing droht bei der Sicherheit die Design-Schwächen des Internets zu erben – und zwar in zweierlei Hinsicht.

Einerseits direkt, nämlich dort wo lokale UC-Systeme mit entfernten Systemen im Internet gekoppelt sind. Hier können sich die Sicherheitsprobleme des klassischen Internets direkt aufs UC auswirken, wenn kein fundamentaler Paradigmenwechsel zur zentralen Bedeutung von sicheren Programmen, Protokollen und Systemen erfolgt.

Andererseits droht UC die schnellen Produktzyklen der heutigen IT zu erben und damit dem ökonomischen Druck zu unterliegen, möglichst schnell scheinbar gut funktionierende Produkte und rasche Marktfähigkeit erreichen zu müssen, ohne sich ausreichend und rechtzeitig um einen gründlichen Prozess des Sicherheits-Engineerings zu bemühen. Dafür ist das Design der einfachen RFID-Tags für den Massenmarkt paradigmatisch, und es steht zu befürchten, dass sich auch in anderen UC-Bereichen wie der Sensornetztechnik ähnliche Fehler wiederholen könnten.

Fundamentale Schwierigkeiten bei den neueren UC-Technologien wie RFID und Sensornetzen ergeben sich aus dem Problem, nur unter größerem Aufwand gute Kryptographie auf den Geräten einsetzen zu können, die der fundamentale Baustein für Sicherheitslösungen

bildet. Hinzu tritt, dass das Problem des kryptographischen Schlüsselmanagement in den offenen Netzen des UC nicht gelöst ist.

Die klassischen Sicherheitsschwächen des Internets und die Mängel der neuen, lokalen Interaktions- und Zugangstechnologien zusammen werden sich dabei im UC nicht einfach addieren, sondern drohen durch den neuartigen, ungekannt hohen Grad an wechselseitiger Vernetzung eine neue Risikodimension der IT-Sicherheit zu erreichen.

Weiterhin ist unsere These, dass ohne Informationssicherheit keine echte Selbstbestimmung im UC möglich ist. IT-Sicherheit ist notwendig, aber nicht hinreichend für informationelle Selbstbestimmung. Die Lösung der Sicherheitsproblematik ist also auch unter diesem Aspekt fundamental, darf aber ihrerseits nicht zu starken neuen Einschränkungen der informationellen Selbstbestimmung führen.

Abstrahiert man von diesen praktischen Problemen einer sicheren Implementierung, kann man dennoch auch auf technische Applikationen blicken, die die informationelle Selbstbestimmung im UC zumindest unterstützen könnten. Verallgemeinerungen von „DRM für Privacy“ und P3P ins UC würden dabei allerdings eine starke (auch internationale) gesetzliche Verankerung benötigen, wobei auch geklärt werden müsste, wer die Kosten etwa einer Einführung von Privacy-DRM tragen sollte. Dort, wo die Daten genutzt werden dürfen, entsteht auch zwangsläufig eine Sicherheitslücke. Ohne intensive, vielleicht teilweise zu automatisierende Kontrolle ihrer Einhaltung und Sanktionen werden gesetzliche Maßnahmen allerdings nicht greifen – eine derartige Kontrolle selbst wiederum könnte sich ihrerseits negativ auf die informationelle Selbstbestimmung auswirken.

Identitätsmanagement im UC stellt eine viel versprechende Forschungsrichtung dar, findet aber gegenüber den Sensoren des UC, die z.B. direkt und unauffällig Körpermerkmale erfassen können, seine Grenzen. Es müsste somit ebenfalls von starken gesetzlichen Maßnahmen flankiert werden, die wiederum zur Durchsetzung ein starkes Audit und entsprechende Sanktionen benötigen.

Weiteres wichtiges Element von Selbstbestimmung im UC, das etwas leichter zu lösen scheint als die Sicherheitsfrage, ist ein hoher Grad an Offenheit von Schnittstellen, Datenformaten, Protokollen und Software, um dem Menschen (oder einem von ihm vertrauten Experten) auf Wunsch Einsicht und stärkere Kontrolle über die UC-Umgebung einzuräumen.

Zentral wird bei jeder UC-Anwendung, die den Menschen betrifft, auch die Frage des Interaktionsparadigmas – kann und wird man das System so gestalten, dass der Mensch der Initiator ist? – und der Auflösung des Gegensatzes von Delegation und Detailkontrolle in flexiblen Schnittstellen zwischen Mensch und UC-System beantwortet werden müssen.

Zusammenfassend lässt sich feststellen, dass die Frage, ob und wie Ubiquitous Computing sicher und selbstbestimmt gestaltet werden kann, noch vollkommen offen ist. Ihre Beantwortung wird vermutlich einen großen Paradigmenwechsel vom „Calm“ zu einem „Secure and Privacy-aware“ Computing erforderlich machen.

7.5 Literatur

Abadi, Martín: Private Authentication. In: Dingledine, Roger / Syverson, Paul, Privacy Enhancing Technologies (PET 2002), Springer, LNCS 2482, 2003, S. 27-40.

Albrecht, Katherine / McIntyre, Liz: Spychips, Nelson Current, 2005.

Anderson, Ross: Security Engineering – A Guide to Building Dependable Distributed Systems. Wiley, New York, 2001.

Anderson, Ross J. / Chan, Haowen / Perrig, Adrian: Key Infection – Smart Trust for Smart Dust, Proceedings of IEEE International Conference on Network Protocols (ICNP 2004), IEEE Computer Society, Oktober 2004, S. 206-215.

Arends, R. / Austein, R. / Larson, M. / Massey, D. / Rose, S.: DNS Security Introduction and Requirements, RFC 4033, März 2005.

Asonov, Dmitri / Freytag, Johann-Christoph: Almost Optimal Private Information Retrieval. In: Dingledine, Roger / Syverson, Paul (Hrsg.): Privacy Enhancing Technologies (PET 2002), Springer, LNCS 2482, 2003, S. 209-223.

Ateniese, Giuseppe / Camenisch, Jan / de Medeiros, Breno: Untraceable RFID tags via Insubvertible Encryption. 12th ACM Conference on Computer and Communications Security – CCS'05, 2005.

Avoine, Gildas / Oechslin, Philippe: RFID Traceability – A Multilayer Problem. In: Patrick, Andrew / Yung, Moti (Hrsg.): Financial Cryptography – FC'05, Roseau, The Commonwealth Of Dominica, Springer, 2005, S. 125-140.

Bauer, Matthias / Fabian, Benjamin / Fischmann, Matthias / Gürses, Seda: Emerging Markets for RFID Traces, in Subm., 2006. http://arxiv.org/abs/cs.CY/0606018 (30.03.2006).

Bauer, Matthias / Meints, Martin / Hansen, Marit (Hrsg.): Structured Overview on Prototypes and Concepts of Identity Management Systems, Deliverable 3.1 of the FIDIS Network of Excellence, 2005, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf (08.03.2006).

Berthold, Oliver: Effizienter unbeobachtbarer Datenbankzugriff. In: Ferstl, Otto K. / Sinz, Elmar J. / Eckert, Sven / Isselhorst, Tilman (Hrsg.): Wirtschaftsinformatik, Physica-Verlag, 2005, S. 1267–1286.

Berthold, Oliver / Günther, Oliver / Spiekermann, Sarah: RFID – Verbraucherängste und Verbraucherschutz, Wirtschaftsinformatik 6 (47), 2005, S. 422-430.

Birman, Kenneth P.: Reliable Distributed Systems – Technologies, Web Services and Applications, Springer, 2005.

Blaß, Erik-Oliver / Zitterbart, Martina: Acceptable Public-Key Encryption in Sensor Networks. In: International Workshop on Ubiquitous Computing, 2005, S. 88-93.

Blaß, Erik-Oliver / Fabian, Benjamin / Fischmann, Matthias / Gürses, Seda F.: Security in Ad-hoc and Sensor Networks, in: Dorothea Wagner and Roger Wattenhofer, Algorithms for Ad-hoc and Sensor Networks, GI/Springer LNCS (in Vorbereitung), 2006.

Bless, R. / Blaß, E.-O. / Conrad, M. / Hof, H.-J. / Kutzner, K. / Mink, S. / Schöller, M.: Sichere Netzwerkkommunikation, Springer, 2005.

Bono, Steve / Green, Matthew / Stubblefield, Adam / Juels, Ari / Rubin, Avi / Szydlo, Michael: Security Analysis of a Cryptographically-Enabled RFID Device, Proceedings USENIX Security Symposium, Baltimore, Maryland, USA, Juli-August 2005, S. 1-16.

Böhme, Rainer / Danezis, George / Diaz, Claudia / Köpsell, Stefan / Pfitzmann, Andreas: On the PET workshop panel – mix cascades versus peer-to-peer: Is one concept superior? In: Martin, David / Serjantov, Andrei (Hrsg.): Privacy Enhancing Technologies (PET 2004), Springer, LNCS 3424, 2005, S. 243-255.

Brickell, Ernie / Camenisch, Jan / Chen, Liqun: Direct Anonymous Attestation. In CCS '04: Proceed-

ings of the 11th ACM Conference on Computer and Communications Security, New York, NY, USA, 2004, ACM Press, S. 132-145.

Bundesamt für Sicherheit in der Informationstechnik (BSI): Risiken und Chancen des Einsatzes von RFID-Systemen, 2004, http://www.bsi.bund.de (06.03.2006).

Burr, William E.: Cryptographic Hash Standards – Where Do We Go from Here? IEEE Security and Privacy, 2(4), 2006, März-April, S. 88-91.

Capkun, Srdjan / Buttyán, Levente / Hubaux, Jean-Pierre: Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, 2(1), 2003, S. 52–64.

Glenn Carl / George Kesidis / Richard R. Brooks / Suresh Rai: Denial-of-Service Attack-Detection Techniques, IEEE Internet Computing, vol. 10, no. 1, 2006, S. 82-89.

Chan, Haowen / Perrig, Adrian: PIKE – Peer Intermediaries for Key Establishment in Sensor Networks, Proceedings of IEEE Infocom, 2005.

Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM (CACM) 2(24) Februar,1981, S. 84-88.

Chaum, David: Security without Identification – Transaction systems to make big brother obsolete, Communications of the ACM CACM, 28(10), Oktober 1985, S. 1030-1044.

Clarke, Ian / Miller, Scott G. / Hong, Theodore W. / Sandberg, Oskar / Wiley. Brandon: Protecting Free Expression Online with Freenet, IEEE Internet Computing, 6(1), Januar-Februar 2002, S. 40-49.

Davenport, Thomas H. / Beck, John C.: The Attention Economy, Harvard Business School Press, Boston, 2001.

Dingledine, Roger / Mathewson, Nick / Syverson, Paul: TOR – The Second-Generation Onion Router, Proceedings of the 13th USENIX Security Symposium, 2004.

Douceur, John R.: The Sybil Attack. In: Revised Papers from the First International Workshop on Peer-to-Peer Systems, Springer, LNCS 2429, 2002, S. 251-260.

Eckert, Claudia: IT-Sicherheit, Oldenbourg Verlag, 3. Auflage, 2004.

Engberg, Stephan / Harning, Morten / Damsgaard Jensen, Christian: Zero-knowledge Device Authentication –Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience, Conference on Privacy, Security and Trust – PST, New Brunswick, Canada, Oktober 2004.

EPCglobal: EPC Radio-Frequency Identity Protocols – Class-1 Generation-2 UHF RFID, 2004.

Eschenauer, Laurent / Gligor, Virgil D.: A key-management scheme for distributed sensor networks, Proceedings of the 9th ACM conference on Computer and communications security (CCS ’02), New York, ACM Press, 2002, S. 41-47.

Evdokimov, Sergei / Fischmann, Matthias / Günther, Oliver: Provable Security for Outsourcing Database Operations, Proceedings of the 22nd International Conference on Data Engineering (ICDE'06), 2006.

Fabian, Benjamin / Günther, Oliver / Spiekermann, Sarah: Security Analysis of the Object Name Service, Proceedings of the 1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2005) in conjunction with IEEE ICPS 2005, Santorini, 2005, S. 71-76.

Feldhofer, Martin / Dominikus, Sandra / Wolkerstorfer, Johannes: Strong Authentication for RFID Systems using the AES Algorithm. In: Joye, Marc / Quisquater, JeanJacques (Hrsg.): Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004 Boston, Springer, 2004, S. 357-370.

Finke, Thomas / Kelter, Harald: Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, 2004, http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf (06.03.2006).

Finkenzeller, Klaus: RFID-Handbuch – Grundlagen und praktische Anwendungen induktiver

Funkanlagen, Transponder und kontaktloser Chipkarten, Carl Hanser Verlag, 3. Auflage, 2002.

Floerkemeier, Christian / Schneider, Roland / Langheinrich, Marc: Scanning with a Purpose – Supporting the Fair Information Principles in RFID protocols. In: Murakami, Hitomi / Nakashima, Hideyuki / Tokuda, Hideyuki / Yasumura, Michiaki (Hrsg.): Ubiquitious Computing Systems – Revised Selected Papers from the 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004) Tokyo 2004, Springer, 2005.

Garfinkel, Simson: Database Nation – The Death of Privacy in the 21st Century, O'Reilly, 2000.

Garfinkel, Simson L.: An RFID Bill of Rights, Technology Review, Oktober 2002, http://www.technologyreview.com/articles/02/10/garfinkel1002.asp (06.03.2006).

Garfinkel, Simson / Juels, Ari / Pappu, Ravi: RFID Privacy – An Overview of Problems and Proposed Solutions, IEEE Security and Privacy, 3, May-June 2005, S. 34-43.

Goldreich, Odred: Foundations of Cryptography, Cambridge University Press, Volume I Basic Tools, 2003 (2001); Volume II Basic Applications, 2004.

Gow, Gordon A.: Privacy and Ubiquitous Network Societies, Background Paper, ITU Workshop on Ubiquitous Network Societies, 2005, http://www.itu.int/osg/spu/ni/ubiquitous/workshop.html (17.03.2006).

Gupta, Vipul / Millard, Matthew / Fung, Stephen / Zhu, Yu / Gura, Nils / Eberle, Hans / Shantz, Sheueling C.: Sizzle – A standards-based end-to-end Security Architecture for the embedded Internet. In: PerCom 2005, Third IEEE International Conference on Pervasive Computing and Communications, 2005, S. 247-256.

Hankerson, Darrel / Menezes, Alfred / Vanstone, Scott: Guide to Elliptic Curve Cryptography, Springer, 2004.

Hansen, Marit / Köhntopp, Kristian / Pfitzmann, Andreas: The Open Source Approach - Opportunities and Limitations with Respect to Security and Privacy; Computers & Security 21/5, 2002, S. 461-471, http://dud.inf.tu-dresden.de/literatur/HaKP_02OpenSource_0214.pdf

Hansen, Marit / Krasemann, Henry / Krause, Christian / Rost, Martin / Genghini, Riccardo: Identity Managements Systems (IMS): Identification and Comparison Study, 2003, http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf (08.03.2006).

Hansen, Marit / Krasemann, Henry (Hrsg.): Privacy and Identity Management for Europe – PRIME White Paper V1, 2005, http://www.prime-project.eu.org/whitepaper/ (10.03.2005).

Hansen, Markus: DRM-Desaster: Das Sony BMG-Rootkit, Datenschutz und Datensicherheit (DuD), 30 (2006), 2, S. 95-97, http://www.datenschutzzentrum.de/drm/DuD(2)2006-Hansen.pdf (13.03.2006).

Hansen, Markus: Ein Zweischneidiges Schwert – Über die Auswirkungen von Trusted Computing auf die Privatsphäre, DANA 03/2004, S. 17-22, http://www.datenschutzzentrum.de/allgemein/trusted_computing.htm (13.03.2006).

Hansen, Markus / Möller, Jan: Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung, in: Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.): IT-Sicherheit geht alle an!, Tagungsband zum 9. Deutschen IT-Sicherheitskongress des BSI, 2005, S. 159-171, http://www.datenschutzzentrum.de/vortraege/050510_hansen-moeller_bsi.htm (13.03.2006).

Hennig, Jan / Ladkin, Peter / Sieker, Bernd: Privacy Enhancing Technology Concepts for RFID Technology Scrutinised, Research Report, RVS-RR-04-02, Universität Bielefeld, Oktober 2004.

Henrici, Dirk / Müller, Paul: Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers. In: Sandhu, Ravi / Thomas, Roshan (Hrsg.): International Workshop on Pervasive Computing and Communication Security – PerSec 2004. Orlando, Florida, IEEE Computer Society, März 2004, S. 149-153.

Henrici, Dirk / Müller, Paul: Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In: Ferscha, Alois / Mattern, Friedemann (Hrsg.): Pervasive Computing: Second Inter-

national Conference, Pervasive 2004, LNCS No. 3001, Springer, 2004, S. 219-224.

Hildebrandt, Mireille / Backhouse, James (Hrsg.): Descriptive Analysis and Inventory of Profiling Practices, Deliverable 7.2 of the FIDIS Network of Excellence, 2005, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.2.profiling_practices.pdf (08.03.2006).

Hilty, Lorenz / Behrendt, Siegfried / Binswanger, Mathias / Bruinink, Arend / Erdmann, Lorenz / Fröhlich, Jürg / Köhler, Andreas / Kuster, Niels / Som, Claudia / Würtenberger, Felix: The Precautionary Principle in the Information Society – Effects of Pervasive Computing on Health and Environment. EMPA, Bern, 2005, http://www.empa.ch/sis (17.03.2006).

Hind, John R. / Mathewson, James M. / Peters, Marcia L.: Identification and tracking of persons using RFID-tagged items, IBM US Patent Application Nr. 20020165758, 2001.

Hubaux, Jean-Pierre / Buttyán, Levente / Capkun, Srdan: The Quest for Security in Mobile Ad Hoc Networks, Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001), 2001.

Iliev, Alexander / Smith, Sean W.: Protecting Client Privacy with Trusted Computing at the Server, IEEE Security and Privacy 2 (3), März-April, 2005, S. 20-28.

Inoue, Sozo / Yasuura, Hiroto: RFID Privacy Using User-controllable Uniqueness, RFID Privacy Workshop, MIT, November 2003.

ISO: Information Processing Systems – OSI Reference Model – Part 2: Security Architecture, Technical Report Nr. 7498-2, 1989.

ISO: Information technology – Security Techniques – Entity Authentication, Technical Report Nr. 9798, 1997/1999.

Juels, Ari: RFID Security and Privacy – A Research Survey, Draft September 2005, in Vorb., IEEE Journal on Selected Areas in Communication, 2006.

Juels, Ari / Pappu, Ravikanth: Squealing Euros – Privacy Protection in RFID-Enabled Banknotes. In: Wright, Rebecca N. (Hrsg.): Financial Cryptography – FC'03, Le Gosier, Guadeloupe, French West Indies, Springer, LNCS 2742, 2003, S. 103-121.

Juels, Ari / Rivest, Ronald / Szydlo, Michael: The Blocker Tag – Selective Blocking of RFID-Tags for Consumer Privacy. In: Atluri, Vijay (Hrsg.): Conference on Computer and Communications Security – ACM CCS, Washington, ACM Press, Oktober 2003, S. 103-111.

Kargl, Frank: Sicherheit in Mobilen Ad hoc Netzwerken, Dissertation, Universität Ulm, 2003.

Karjoth, Günter: Applications of RFID, Vortrag ETH Zürich, Mai 2005 http://www.ifi.unizh.ch/im/imrg/fileadmin/files/Ringvorlesung_UniZurich_30.05.05_Guenter_Karjoth.pdf (06.03.2006).

Karjoth, Günter / Moskowitz, Paul: Disabling RFID-Tags with Visible Confirmation – Clipped Tags Are Silenced, Workshop on Privacy in the Electronic Society – WPES, Alexandria, Virginia, USA, ACM Press, November 2005.

Kesdogan, Dogan / Borning, Mark / Schmeink, Michael: Unobservable surfing on the World Wide Web: Is private information retrieval an alternative to the mix based approach? In: Dingledine, Roger / Syverson, Paul, Privacy Enhancing Technologies (PET 2002), Springer, LNCS 2482, 2003, S. 224-238.

Khalili, Aram / Katz, Jonathan / Arbaugh, William A.: Toward Secure Key Distribution in Truly Ad-Hoc Networks, Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT-w'03), 2003.

Kohno, Tadayoshi / Broido, Andre / Claffy, K.C.: Remote Physical Device Fingerprinting, IEEE Transactions on Dependable and Secure Computing 2 (2005), April – Juni, Nr. 2, S. 93-108.

Krawczyk, H. / Bellare, M. / Canetti, R.: RFC 2104 – HMAC: Keyed-Hashing for Message Authentication, 1997.

Kügler, Dennis: Digitale Sicherheitsmerkmale im elektronischen Reisepass, BSI-Kongress 2005, http://www.kes.info/archiv/material/bsikongress2005/EU-Pass.pdf (06.03.2006).

Kügler, Dennis: On the Anonymity of Banknotes, in: Martin, David / Serjantov, Andrei (Hrsg.), Privacy Enhancing Technologies (PET 2004), LNCS 3424, Springer, 2005.

Langheinrich, Marc: A Privacy Awareness System for Ubiquitous Computing Environments. In: Borriello, Gaetano / Holmquist, Lars E. (Hrsg.): 4th International Conference on Ubiquitous Computing (Ubicomp 2002), Springer, Berlin – Heidelberg, September 2002 (LNCS 2498), S. 237-245.

Langheinrich, Marc: Personal Privacy in Ubiquitous Computing – Tools and System Support. Dissertation, ETH Zürich, Mai 2005.

Langheinrich, Marc: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. In: Fleisch, Elgar / Mattern, Friedemann (Hrsg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, Springer, Berlin – Heidelberg, 2005.

Liberty Alliance: Liberty Specs Tutorial, 2003, http://www.projectliberty.org/ (06.03.2006).

Menezes, Alfred J. / Oorschot, Paul C. / Vanstone, Scott A.: Handbook of Applied Cryptography, CRC Press, 1997.

Microsoft Corporation, Ping Identity Corporation: A Guide to Integrating with InfoCard v1.0, August 2005, http://www.microsoft.com/ (06.03.2006).

Molnar, David / Soppera, Andrea / Wagner, David: Privacy for RFID Through Trusted Computing, Workshop on Privacy in the Electronic Society – WPES, Alexandria, Virginia, USA, ACM Press, November 2005.

OECD: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, September 1980.

Ohkubo, Miyako / Suzuki, Koutarou / Kinoshita, Shingo: Cryptographic Approach to “Privacy-Friendly” Tags, RFID Privacy Workshop, MIT, November 2003.

Ohkubo, Miyako / Suzuki, Koutarou / Kinoshita, Shingo: Efficient Hash-Chain Based RFID Privacy Protection Scheme, International Conference on Ubiquitous Computing – Ubicomp, Workshop Privacy: Current Status and Future Directions, Nottingham, England, September 2004.

Ohkubo, Miyako / Suzuki, Koutarou / Kinoshita, Shingo: RFID privacy issues and technical challenges, Communications of the ACM (CACM) 48 (9), September 2005, S. 66-71.

Pering, Trevor / Ballagas, Rafael / Want, Roy: Spontaneous marriages of mobile devices and interactive spaces, Communications of the ACM (CACM) 48 (9), September 2005, S. 53-59.

Pfitzmann, Andreas: Werden biometrische Sicherheitstechnologien die heutige IT-Sicherheitsdebatte vor neue Herausforderungen stellen?, Vortrag 2005, http://dud.inf.tu-dresden.de/literatur/BiometrieRFID.pdf (03.06.2006).

Ranganathan, Kumar: Trustworthy Pervasive Computing – The Hard Security Problems, Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), IEEE Computer Society, 2004.

Rieback, Melanie / Crispo, Bruno / Tanenbaum, Andrew: RFID Guardian: A battery-powered mobile device for RFID privacy management. In: Boyd, Colin / Nieto, J. M. G. (Hrsg.): Australasian Conference on Information Security and Privacy – ACISP’05 Brisbane (Australia), Springer, LNCS 3574, S. 184-194.

Rieback, Melanie / Crispo, Bruno / Tanenbaum, Andrew: Is Your Cat Infected with a Computer Virus? In: Proc. 4th IEEE Intl. Conf. on Pervasive Computing and Communications (PerCom 2006), Pisa, Italy, März 2006.

Rieback, Melanie / Crispo, Bruno / Tanenbaum, Andrew: The Evolution of RFID Security. IEEE Pervasive Computing, 5(1), 2006, S. 62-69.

Salzmann, Thomas: En passant – Funktechnologie im kommunalen Einsatz, iX 4, 2006, S. 112-114.

Schneier, Bruce: Attack Trees, Dr. Dobb's Journal, Dezember 1999.

Shirey, R.: RFC 2828 – Internet Security Glossary, 2000.

Sieker, Bernd / Ladkin, Peter B. / Hennig, Jan E.: Privacy Checklist for Privacy Enhancing Technology Concepts for RFID Technology Revisited, Oktober 2005.

Soliman, Hesham: Mobile IPv6, Addison-Wesley, 2004.

Spiekermann, Sarah / Ziekow, Holger: Technische Analyse RFID-bezogener Angstszenarien, Working Paper, November 2004.

Stajano, Frank: Security for Ubiquitous Computing, John Wiley & Sons, Chichester (UK), 2002.

Stajano, Frank: RFID is X-ray vision, Technical Report, University of Cambridge, Computer Laboratory (UCAM-CL-TR-645), 2005.

Stajano, Frank: RFID is X-Ray Vision, Communications of the ACM (CACM) 48 (9), 2005, S. 31-33.

Stallings, William: Cryptography and Network Security, Prentice-Hall, 3rd ed., 2002.

Steinmetz, Ralf / Wehrle, Klaus (Hrsg.): Peer-to-Peer Systems and Applications, Springer, LNCS 3485, 2005.

SWAMI Project – Safeguards in a World of Ambient Intelligence: http://swami.jrc.es/pages/ (17.03.2006).

UBISEC Project – Ubiquitous Networks with a Secure Provision of Services, Access, and Content Delivery: http://jerry.c-lab.de/ubisec/ (17.03.2006).

W3C: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, Juli 2005, http://www.w3.org/TR/2005/WD-P3P11-20050701/ (06.03.2006).

Walters, J. P. / Liang, Z. / Shi, W. / Chaudhary, V.: Wireless Sensor Network Security – A Survey, 2005, http://www.cs.wayne.edu/%7Eweisong/papers/walters05-wsn-security-survey.pdf (06.03.2006).

Weis, Stephen A.: Security and Privacy in Radio-Frequency Identification Devices. Master Thesis, Cambridge, MA 02139, Massachusetts Institute of Technology, Mai 2003.

Weis, Stephen A. / Sarma, Sanjay E. / Rivest, Ronald L. / Engels, Daniel W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter, Dieter, et al. (Hrsg.): Security in Pervasive Computing (SPC 2003), Springer, Berlin - Heidelberg, 2004 (LNCS 2802), S. 201-212.

Weiser, Mark: The Computer for the 21st Century, Scientific American 265, 1991, S. 66-75.

Weiser, Mark: Some Computer Science Problems in Ubiquitous Computing, Communications of the ACM (CACM) 36 (7), 1993, S. 75-84.

Weiser, Mark / Brown, John S.: The Coming Age of Calm Technology, 1996, http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm (06.03.2006).

Yamada, S. / Kamioka, E.: Access Control for Security and Privacy in Ubiquitous Computing Environments, IEICE Trans. Commun. Bd. E88-B(3), 2005.

Zhou, Lidong / Haas, Zygmunt J.: Securing Ad Hoc Networks, IEEE Network 6 (13), 1999, S. 24-30.

Zhou, Dan: Security Issues in Ad Hoc Networks. In: Ilyas, Mohammad (Hrsg.): The Handbook of Ad Hoc Wireless Networks, CRC Press, 2003.

8 Zusammenfassung der Ergebnisse

8.1 Rechtliche Möglichkeiten des Risikomanagements

Viele der durch UC-Systeme aufgeworfenen Rechtsprobleme sind nicht grundlegend neu, sie werden durch die Verbreitung von UC-Systemen aber zusätzlich verschärft. Ihre Wurzeln liegen in der fortschreitenden Miniaturisierung und Vernetzung der Verarbeitung personenbezogener Daten begründet, die mit der Entwicklung von verteilten und vernetzten UC-Anwendungen eine weitere Stufe erreicht. Die Probleme eines wirksamen Datenschutzes für UC-Anwendungen werden durch die Verlagerung von Verarbeitungsschritten in andere Länder, insbesondere unsichere Drittstaaten, noch weiter vertieft. Folgende wesentliche Risiken und Möglichkeiten des Risikomanagements ergeben sich im Einzelnen.

8.1.1 Rechtsdurchsetzung

Für den Betroffenen ist die Geltendmachung seiner Rechte nur attraktiv, wenn diese mit angemessenem Aufwand möglich und kurzfristig verfügbar ist und kein übermäßiges Kostenrisiko bedeutet. Insbesondere der Zeitfaktor wird angesichts der Vielzahl permanent stattfindender Verarbeitungen und der zu erwartenden Innovationsgeschwindigkeit von UC-Systemen für einen effektiven Rechtsschutz bedeutend sein.

Die Durchsetzung der Datenschutzrechte zu Gunsten der Betroffenen kann erheblich verbessert werden, wenn das Eigeninteresse der Betreiber von UC-Systemen gestärkt und die Abhängigkeit von dem Vollzugsdefizit im Datenschutz reduziert wird. Dies lässt sich z.B. durch die Einführung einer nutzerzentrierten Gefährdungshaftung der Betreiber von UC-Systemen erreichen. Voraussetzung ist jedoch die Einführung eines Anspruches auf Ersatz eines immateriellen Schadens für die Verletzung des informationellen Selbstbestimmungsrechts bzw. des Persönlichkeitsrechts des Betroffenen.

8.1.2 Datensparsame Technikgestaltung

Vorbeugende Schutzmaßnahmen werden eine wesentliche Rolle für den Datenschutz in UC-Systemen spielen müssen. Dazu gehört eine datensparsame zweckorientierte Technikgestaltung ebenso wie datenschutzfreundliche Voreinstellungen von Anwendungen in UC-Systemen. Sie ergeben sich aus der Verpflichtung zur Wahrung der gesetzlich geregelten Datenschutzrechte und können durch ökonomische Erwägungen der Betreiber von UC-Systemen unterstützt werden. Die UC-Betreiber können durch die Nachfrage der Kunden und Verbraucher nach datenschutzfreundlichen UC-Anwendungen angeregt werden. Für sie kann aber auch von Bedeutung sein, dass sich das Risiko von Persönlichkeitsverletzungen aus dem Betrieb ihres UC-Systems in Haftungsrisiken niederschlägt, denen es durch eine datenschutzkonforme Technikgestaltung und –anwendung vorzubeugen gilt. Müssen diese durch Versicherungen abgedeckt werden, entsteht eine zusätzliche Motivation, die zum Be-

trieb datenschutzfreundlicher UC-Produkte und Dienstleistungen beiträgt.

8.1.3 Zweckbindung

Der datenschutzrechtliche Grundsatz der Zweckbindung ist für die Verarbeitung personenbezogener Daten in UC-Systemen von erheblicher Bedeutung, da sie eine umfassende Profilbildung über das Verhalten des Betroffenen ermöglichen. Solche Profile haben im Regelfall einen großen wirtschaftlichen Wert, so dass ein entsprechendes Verwertungsinteresse grundsätzlich in die Risikobetrachtung einbezogen werden muss. Die Generierung und Verwendung von Nutzungs- und Verhaltensprofilen aus UC-Systemen ist ohne eine ausdrückliche Zustimmung des Betroffenen rechtswidrig. Angesichts der gegenläufigen wirtschaftlichen Interessen sollte eine rechtswidrige Verarbeitung und Nutzung der im Rahmen von in UC-Systemen entstandenen Profildaten deutlich sanktioniert werden. Dies wäre de lege lata über Regelungen zum Strafschadensersatz möglich, aber auch durch eine normenklare Sanktionierung entsprechender Normverstöße in die datenschutzrechtlichen Bußgeldtatbestände bzw. bei einer entsprechenden Bereicherungsabsicht auch in die Strafvorschriften. Die Rechtsdurchsetzung liegt im Übrigen in den Händen der Aufsichtsbehörden, deren wirksame Tätigkeit eine entsprechende personelle Ausstattung voraussetzt.

8.1.4 Transparenz

Datenschutzrechtlich ist den Betroffenen eine umfassende Transparenz der Verarbeitungsvorgänge ihrer Daten in UC-Systemen zu gewährleisten. Insbesondere weil eine Vielzahl unsichtbarer und parallel stattfindender Verarbeitungen eine detaillierte Information im Einzelfall kaum zulassen wird (Ökonomie der Aufmerksamkeit), gewinnt eine verständliche und nachvollziehbare Aufklärung bspw. über die systematischen Zusammenhänge der Verarbeitungen und der verwendeten Daten und Kriterien innerhalb bestimmter räumlicher Bereiche und begrenzter Zeithorizonte an Bedeutung. Derartige systematische Unterrichtungen werden in UC-Systemen die Wissensbasis für selbstbestimmte Entscheidungen des Betroffenen bilden müssen.

Der Betroffene muss aber nicht nur unterrichtet werden, sondern er muss auch seinen Auskunftsanspruch wirksam wahrnehmen können. Hierzu ist ihm in Anlehnung an die Angebote bestehender Onlinedienste die Möglichkeit zu geben, vor Ort, über das Internet oder andere ihm ohne weiteren Aufwand erreichbare Mittel, ein „Datenkonto“ mit den über ihn im Rahmen des UC-Systems zu seiner Person verarbeiteten Daten bereit zu stellen. Er sollte darüber hinaus über die Möglichkeit verfügen, personenbeziehbare Objektdaten aus der Nutzung des UC-Systems zu löschen. Die Betreiber eines UC-Systems haben die Betroffenen auf den Betrieb von Lesegeräten bzw. Sensoren hinzuweisen und eine Stelle anzugeben, an die sie sich zur Wahrnehmung ihrer Datenschutzrechte wenden können.

8.1.5 Verantwortlichkeiten

Der räumliche und zeitliche Einsatz von UC-Anwendungen erfordert finanzielle Aufwendungen, über die in Organisationen die verantwortlichen Entscheidungsträger zu befinden haben. Verantwortlich für die Rechtmäßigkeit der Erhebung von personenbeziehbaren Objektdaten ist im Regelfall der Betreiber des Hintergrundsystems, in dem die Lesegeräte und Sensoren miteinander verknüpft sind. Dieser wird im Regelfall personenbezogene Daten in definierten „Räumen" für eigene Zwecke erheben und verarbeiten und trägt insoweit auch die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung. Neben dem für das Hintergrundsystem Verantwortlichen kommt auch der Inhaber des Hausrechts als Verantwortlicher in Betracht, wenn er eine heimliche oder offene Erhebung personenbeziehbarer Objektdaten veranlasst oder in seinen Räumlichkeiten duldet. Werden personenbezogene Daten auf den Mikrochips der Objekte gespeichert, dann sind in Anlehnung an § 6 c Abs. 1 BDSG die Stellen für die Datenverarbeitung verantwortlich, die den Datenträger ausgegeben bzw. ihn programmiert haben.

8.1.6 Internationalität und Outsourcing

Erfolgt die Datenverarbeitung in UC-Systemen durch Betreiber mit Sitz in mehreren Ländern, so ist sie für das Gesamtsystem mangels eines international einheitlichen Datenschutzstandards auf das nach der EG-Datenschutzrichtlinie zulässige Schutzniveau zu begrenzen. Die Kontrolle und Durchsetzung dieser Anforderung wird angesichts des Umfangs der Verarbeitungen und der nur begrenzten Möglichkeiten einer einfachen Rechtsdurchsetzung im Ausland, insbesondere angesichts der bestehenden Vollzugsdefizite im Datenschutz, problematisch bleiben.

8.1.7 Rechtliche Rahmenbedingungen technischer Schutzmechanismen

Eine zentrale Rolle zur Vermeidung von Datenschutzrisiken wird der Entwicklung und Implementierung von Mechanismen des Identitätsmanagements zukommen, das die Betroffenen u.a. bei der Abgabe und Verwaltung von Einwilligungserklärungen unterstützt. Kombiniert mit Pseudonymitätskonzepten sollte es Ziel einer solchen Gestaltung sein, die Verarbeitung personenbezogener Objektdaten durch zusätzliche Schutzmechanismen zu ermöglichen, ohne die informationelle Selbstbestimmung der Betroffenen zu gefährden.

Zur Förderung und Implementierung derartiger Mechanismen bedarf es flankierender normativer Maßnahmen. Hierzu gehören neben Anforderungen der Standardisierung und der Interoperabilität, die ein Identitätsmanagement über Produkt- und Herstellergrenzen hinweg ermöglichen, auch Regelungen, die den maschinell unterstützten Einwilligungserklärungen nicht nur eine bindende Wirkung zukommen lassen, sondern auch ihre Einhaltung kontrollieren können. Eine solche Rechtssicherheit bspw. für die Wirksamkeit von Einwilligungserklärungen, die mit Unterstützung eines Identitätsmanagers erteilt werden, wird sich auch positiv auf die Akzeptanz solcher Systeme bei den Nutzern von UC-Systemen auswirken.

Eine Automatisierung der Kontrolle datenschutzrechtlicher Vorgaben kann nachhaltig zu einer verbesserten Durchsetzung der Datenschutzrechte und damit zu einer Reduzierung des faktischen Vollzugsdefizits im Datenschutz beitragen. Wenn persönliche Daten umfassend in UC-Systemen verarbeitet werden, stellt eine solche Automatisierung eine wichtige Möglichkeit dar, Kontrollen durch die verantwortlichen Stellen selbst, die Betroffenen oder die Aufsichtbehörden in nennenswertem Umfang und wirtschaftlich tragbar zu realisieren. Wirksame Kontrollen und Rechtsdurchsetzung fördern einen faktischen Datenschutzstandard unmittelbar. Automatisiertes Datenschutzmanagement erfordert neben einer standardisierten technischen Plattform für den Austausch von Metainformationen auch maschinenlesbare Datenschutzrichtlinien, die die rechtlichen Anforderungen erfüllen.

8.2 Wirtschaft und Soziales

Informations-, Kommunikations- und Automatisierungsdienste, die über UC-Technologie immer häufiger zum Einsatz kommen, werden von Verbrauchern relativ positiv bewertet. Insbesondere werden Dienstleistungen geschätzt, die zu einer Zeitersparnis führen oder dabei helfen, Produktrisiken zu reduzieren.

Allerdings scheint diese positive Beurteilung in einem Spannungsverhältnis zu einem potenziellen Kontrollverlust zu stehen. Dieser Kontrollverlust kann zum einen in einer Aufgabe der informationellen Selbstbestimmung liegen; z.B. wenn RFID-Lesegeräte unbemerkt auf Chips in den eigenen Gegenständen zugreifen. Zum anderen kann das autonome Handeln von intelligenten Objekten zu einem physischen Kontrollverlust führen.

Beide Arten von Kontrollverlust führen bei den befragten Verbrauchern zu einer reduzierten Neigung, UC-Dienstleistungen in Anspruch zu nehmen.

Es ist daher aus ökonomischer Sicht sinnvoll, Verbraucherbedenken proaktiv zu begegnen und ihnen eine effektive Kontrolle über angebotene UC-Dienstleistungen und ihre Risiken einzuräumen. Diese sollte objektiv wirksam und leicht vermittelbar sein, denn komplexen technischen Implementierungen zum Schutz der Privatsphäre wird – so legen es einige Untersuchungen nahe – wenig vertraut (evtl. auch aufgrund von Unverständnis).

Die Untersuchungen zur Wahrnehmung von Datenverarbeitung und Datenschutz legen nahe, dass ein nicht unbedeutender Teil der deutschen Verbraucher sehr wenig Verständnis dafür hat, was Datenverarbeitung bedeutet. Die Mehrheit scheint zwar um die Existenz einer kommerziellen Datenverarbeitung zu wissen. Die sich daraus ergebenden Konsequenzen scheinen dem Einzelnen meistens wenig transparent zu sein. Insgesamt wird an ein hohes Schutzniveau durch Gesetze geglaubt. Ein Vertrauen, das – einmal auf's Spiel gesetzt - in ein grundlegendes Misstrauen umschlagen könnte. Eine diskriminierende Nutzung von Informationen, wie sie sich z.B. in der bevorzugten Behandlung besonders guter Kunden niederschlägt, wird von der Mehrheit weder erwartet noch gewünscht.

8.3 Sicherheitstechnische Perspektiven

8.3.1 Sicherheit im Ubiquitous Computing

Die Entwicklung von technischen und organisatorischen Lösungen zum Schutz der informationellen Selbstbestimmung des Individuums im Ubiquitous Computing (UC) steht noch am Anfang. Von zentraler Bedeutung ist, wie IT-Sicherheit im UC geplant und umgesetzt wird, aber auch, an welche Grenzen sie stößt.

Ubiquitous Computing droht im Bereich der Sicherheit die Entwurfsschwächen des Internets zu erben – und zwar in zweierlei Hinsicht. Einerseits direkt, nämlich dort, wo lokale UC-Systeme mit entfernten Systemen per Internet gekoppelt sind. Hier können sich die notorischen Sicherheitsprobleme des klassischen Internets direkt auf UC auswirken, wenn kein durchgreifender Paradigmenwechsel zur Entwicklung und Anwendung von sicheren Programmen, Protokollen und Systemen erfolgt.

Andererseits droht UC die schnellen Produktzyklen der heutigen IT zu erben und damit dem ökonomischen Druck zu unterliegen, möglichst schnell scheinbar gut funktionierende Produkte und rasche Marktfähigkeit erreichen zu müssen, ohne ausreichend und rechtzeitig einem gründlichen Prozess des Sicherheits-Engineering oder der Qualitätssicherung unterzogen worden zu sein. Paradigmatisch für eine negative Entwicklung ist der Entwurf der einfachen RFID-Tags für den Massenmarkt. Es steht zu befürchten, dass sich auch in anderen UC-Bereichen wie der Sensornetztechnik ähnliche Fehler wiederholen könnten.

Grundlegende Schwierigkeiten bei den neueren UC-Technologien wie RFID und Sensornetzen ergeben sich aus dem Problem, nur unter größerem Aufwand „gute“ Kryptographie auf den Geräten einsetzen zu können, die den fundamentalen Baustein für Sicherheitslösungen bilden. Hinzu kommt, dass das Problem des kryptographischen Schlüsselmanagements in den offenen Netzen des UC nicht gelöst ist.

Die klassischen Sicherheitsschwächen des Internets und die Mängel der neuen, lokalen Interaktions- und Zugangstechnologien zusammen werden sich im UC voraussichtlich nicht einfach addieren, sondern drohen durch den neuartigen, ungekannt hohen Grad an wechselseitiger Vernetzung eine neue Risikodimension der IT-Sicherheit zu erreichen. Insbesondere Dienste, deren Konzepte auf der Bildung von Profilen basieren, stellen eine gravierende Gefährdung für die Sicherheit und Privatsphäre der Nutzer dar.

Unsere These ist, dass ohne Informationssicherheit keine echte Selbstbestimmung im UC möglich ist. IT-Sicherheit ist notwendig, aber nicht hinreichend für die informationelle Selbstbestimmung. Die Lösung der Sicherheitsproblematik ist also auch unter diesem Aspekt fundamental, darf aber ihrerseits nicht zu neuen Einschränkungen der informationellen Selbstbestimmung führen.

Identitätsmanagement im UC stellt eine viel versprechende Forschungsrichtung zur Lösung von Datenschutzfragen dar. Es findet aber gegenüber den Sensoren des UC, die z.B. direkt und unauffällig Körpermerkmale erfassen können, seine Grenzen. Um wirksam zu sein,

müssen derartige Mechanismen von gesetzlichen Maßnahmen flankiert werden, ihre Durchsetzung bedarf starker Kontrollmechanismen wie Auditverfahren sowie entsprechender Sanktionen, wenn die Schutzmechanismen zu Lasten der Betroffenen unterlaufen werden.

Ein wichtiges Element zur Gewährleistung von Selbstbestimmung im UC ist ein hoher Grad an Offenheit von Schnittstellen, Datenformaten, Protokollen und Software, um dem Betroffenen (oder einem von ihm vertrauten Experten) auf Wunsch Einsicht und Kontrolle über die UC-Umgebung einzuräumen.

Zentral wird bei jeder UC-Anwendung, die den Menschen betrifft, die Frage des Interaktionsparadigmas sein, d.h. ob die Gestaltung der UC-Systeme den Menschen als Initiator der Prozesse in den Mittelpunkt stellen kann und wird und ob und gegebenenfalls wie sich der Gegensatz zwischen Delegation und Detailkontrolle in flexiblen Schnittstellen zwischen Mensch und UC-System umsetzen lassen wird.

Zusammenfassend lässt sich feststellen, dass die Frage, ob und wie Ubiquitous Computing technisch sicher und selbstbestimmt gestaltet werden kann, noch vollkommen offen ist.

8.3.2 Sicherheit bei RFID

Die Suche nach Lösungen für Informationssicherheit und informationelle Selbstbestimmung in RFID-Systemen ist ein vollkommen offenes Forschungsgebiet. Eine Hauptursache ist die Unverträglichkeit eines globalen und allgegenwärtigen Identifikationssystems für Objekte mit der informationellen Selbstbestimmung der individuellen Objekt-Besitzer. Eine zweite Ursache ist der Verzicht auf jegliche Sicherheitsmechanismen in den Plänen der Systembetreiber. Dieser klassische Designfehler, Sicherheit und Datenschutz als nachträglichen „Patch“ und nicht als fundamentalen Bestandteil einer gründlichen Ingenieurskunst zu betrachten, hat im Fall RFID als negatives Beispiel Lehrbuchcharakter.

Selbst unter der Voraussetzung, dass auf allen Tags im Privatbesitz kryptographische Hashfunktionen oder symmetrische Verschlüsselungsverfahren eingesetzt werden könnten, resultierte daraus keineswegs sofort ein sicheres Gesamtsystem. Ferner sind alle Verfahren ungeeignet, die erst über der MAC-Schicht ansetzen und Identifikatoren für die Antikollisionsprotokolle unverändert lassen, da sie ein Tracking und ein Auslesen des Besitzes nicht verhindern.

Für geschlossene Systeme mit einem kleinen, vorher bekannten Teilnehmerkreis und einer begrenzten Anzahl von Tags zeichnen sich Lösungen ab. Nicht jedoch für offene Systeme, die z.B. auch Dienste nach dem Verlauf eines Objektes („Post-Sale Services“) anbieten und dabei etwa auch das geplante globale EPC-Netzwerk einbinden. Alle Verfahren müssen um ein sicheres Verfahren zum Schlüsselmanagement ergänzt werden – ein Problem, das derzeit noch nicht einmal theoretisch gelöst ist. Verwendet man dazu ein portables Master-Gerät wie ein Smart-Phone oder einen PDA, werden die hierfür verwendeten Kommunikationsprotokolle und Applikationen neue, über das Internet ausnutzbare Verwundbarkeiten schaffen.

Ohne einfache, d.h. vom normalen Nutzer durchführbare Verfahren zum Rückruf von Schlüsseln in den Tags sind alle betrachteten technischen Lösungen nicht dauerhaft sicher. Unter dem Gesichtspunkt der Benutzerfreundlichkeit dürfen Nutzer nicht von den Verfahren zum Schutz ihrer Privatsphäre überfordert werden, weil sonst scheinbar „störende" Komponenten – wie z.B. das Benutzen verschiedener Passwörter – umgangen werden und das System versagt.

Die Möglichkeiten heimlich über eine Funkschnittstelle Daten zu sammeln und zur Profilbildung zu verwenden, lassen sich unter den gegebenen Bedingungen mit rein technischen Mitteln nicht wirksam unterbinden. Ebenso wenig lässt sich mit rein technischen Instrumenten gewährleisten, dass Informationen, die einem Dienstanbieter autorisiert zur Verfügung gestellt worden sind, von ihm entgegen ihrer Zweckbindung verwendet oder an Dritte weitergeleitet werden. Hier helfen letztlich nur datenschutzrechtliche Verpflichtungen, die auch wirksam durchgesetzt werden müssen. Dabei ist stets situationsabhängig zu prüfen, ob angesichts des Wertes der Daten Selbstverpflichtungen der Betreiber von UC-Systemen den Betroffenen einen ausreichenden Schutz bieten können.

Das Problem der Informationssicherheit und des Schutzes der Privatsphäre in RFID-gestützten UC-Umgebungen ist nach der derzeitigen Lage als ungelöst zu betrachten. Solange das Paradigma der Kostenminimierung bei der Herstellung und Implementierung der Tags dominiert, erscheint es höchst zweifelhaft, ob eine unter Datenschutzgesichtspunkten befriedigende Lösung in absehbarer Zeit zu erwarten ist. Eine unter technischen Gesichtspunkten ausreichend sichere Gestaltung wird unter diesen Voraussetzungen erheblicher Anstrengungen bedürfen.

8.3.3 Offenheit und Aufmerksamkeitsökonomie

Voraussetzung für die Entwicklung datenschutzgerechter UC-Systeme sind verschiedene Aspekte von Offenheit, die es zu fördern gilt. Offene Standards für UC-Technologie, d.h. insbesondere auch Standards, die einfach und möglichst unentgeltlich von jedermann genutzt werden können, erhöhen neben der Interoperabilität von UC-Systemen auch die Transparenz der Systeme. Diese stellt eine notwendige Bedingung für die Kontrolle durch den Nutzer und seine Selbstbestimmung dar.

Um offene Standards für UC zu erreichen, erscheinen die Entwicklung und der Einsatz von Open Source-Software als attraktive Option, vorausgesetzt dies lässt sich mit den Geschäftsmodellen der Hersteller und Betreiber vereinbaren. Mit Open Source ließen sich potenziell auch Transparenz und Modifizierbarkeit insbesondere lokal eingesetzter UC-Technologie gewährleisten.

Erforderlich ist aber ebenfalls die Transparenz der Datenflüsse, der Datenhaltung und der Datenauswertung, was nicht nur durch die Auswahl einer Technologie erreicht werden kann, sondern durch organisatorische und gesetzliche Rahmenbedingungen unterstützt werden muss.

Schließlich gehört zur Gewährleistung der Selbstbestimmung im UC ein offener Zugang zu

seinen Systemen und dem damit verbundenen Nutzen. Einerseits müssen UC-Systeme die Bedürfnisse gesellschaftlicher Minderheiten wie z.B. behinderter Menschen berücksichtigen. Dies darf jedoch nicht an mangelnder Übereinstimmung eines Kontextes mit einer wie auch immer definierten „Norm“ scheitern. Andererseits bietet das enorme Volumen an gesammelten Daten die Gelegenheit zu noch ungeahnter Personalisierung, und einer Diskriminierung der Nutzer. Besonders für den letzten Aspekt fehlen wirksame technische Lösungsansätze, die die rechtlichen Normen effektiv unterstützen.

Zentral für die Gestaltung von UC-Anwendungen wird sein, den Menschen als Initiator der Interaktionen innerhalb der Anwendung in den Mittelpunkt zu stellen, damit die Interaktionen der Objekte über ihn nicht ohne seine aktive Mitwirkung möglich sind.

8.3.4 Fazit

Die Frage, ob und wie Ubiquitous Computing sicher und im Sinne des Datenschutzes selbstbestimmt gestaltet werden kann, ist noch unbeantwortet. Die Gestaltung datenschutzgerechter UC-Systeme wird noch erheblicher technischer Anstrengungen in Forschung und Entwicklung bedürfen.[741] Eine umfassende Lösung wird einen grundlegenden Paradigmenwechsel vom „Calm“ zum „Secure and Privacy Aware“ Computing erforderlich machen, ohne dass dies die informationelle Selbstbestimmung beeinträchtigen darf.

[741] Empfehlungen für Forschung und Entwicklung siehe unten Kapitel 9.3.

9 Handlungsempfehlungen zur Gewährleistung der informationellen Selbstbestimmung im UC

9.1 Designempfehlungen für UC-Systeme

UC-Systeme müssen zur Wahrung der informationellen Selbstbestimmung und aus Akzeptanzgründen so gestaltet sein, dass ihre Nutzer die Kontrolle und Steuerung über die Verarbeitungsprozesse ihrer Daten wahrnehmen können. Objekte sollten dem Nutzer nur so viel Kontrolle über die Verarbeitungsprozesse abnehmen, wie dieser explizit an den Betreiber eines Systems delegiert hat. Eine implizite Delegation im Wege einer Grundeinstellung des Systems setzt voraus, dass der Nutzer über ihre Funktionalität sowie über die Verarbeitungsprozesse informiert wird. Der Nutzer muss stets Kontrolle über die Aktionen seiner Objekte ausüben können. Das „letzte Wort“ darf dem Nutzer nicht von intelligenten Diensten entzogen werden.

Anonymität und Datensparsamkeit müssen als Standardvoreinstellungen in allen Systemen verankert werden. UC-Systeme sollten nur die unmittelbar zur Erbringung eines Dienstes erforderlichen Daten erheben und diese unmittelbar nach Erreichung des Primärzwecks wieder löschen. Andere Verwendungszwecke sowie weitergehende personenbezogene Datenerhebungen und –verarbeitungen bedürfen einer Einwilligung des Betroffenen. In Anlehnung an bestehende Onlinedienste ist dem Betroffenen die Möglichkeit zu geben, vor Ort, über das Internet oder andere ihm ohne weiteren Aufwand erreichbare Wege, sein Kundendatenkonto einzusehen und seine UC-Daten aus dem System zu löschen.

Für das Auslesen von RFID-Tags in öffentlichen oder öffentlich-zugänglichen Räumen sollten grundsätzlich folgende Einschränkungen gelten:

- RFID-Tags sind durch eine gesonderte Kennzeichnung sichtbar.
- Der Electronic Product Code darf nur ohne Seriennummer des Objekts ausgelesen werden.
- Die Zeitstempelgenauigkeit ist beschränkt, sodass keine sozialen Netzwerkanalysen auf Basis von RFID-Daten durchgeführt werden können.
- Gewonnene Zeit- und Ortsinformationen von Einlesungen müssen unmittelbar nach Erreichung des Primärzwecks, bei vorliegenden Einwilligungen nach Durchführung der umfassten Verarbeitungen gelöscht werden.
- Daten, die dezentral von Lesegeräten gesammelt werden, dürfen auch nur dezentral ausgewertet und nicht personenbezogen auf einer höheren Ebene aggregiert und ausgewertet werden.
- Betreiber von RFID-Infrastrukturen haben die Pflicht, auf den Betrieb von Lesegeräten hinzuweisen und eine Stelle anzugeben, an die sich ein Nutzer zur Wahrnehmung seiner Datenschutzrechte (z.B. auf Auskunft, Berichtigung oder Löschung seiner in der jeweiligen Infrastruktur erhobenen und gespeicherten Daten) wenden kann.

Personenbezogene Datenverarbeitungen in UC-Systemen müssen sich auf das für die Diensterbringung gegenüber dem Betroffenen erforderliche Maß beschränken und dies gegenüber dem Kunden transparent machen. Dazu gehören insbesondere Informationen über Art und Umfang der erhobenen Daten, ihren Verwendungszweck, eventuelle Empfänger sowie Auftragsdatenverarbeiter. Letzteres muss in gleicher Weise für weitergehende Datenverarbeitungen gelten, die auf der Basis einer Einwilligung des Nutzers erfolgen. Der Nutzer muss seine Datenschutzrechte auf einfache Art und Weise und ohne Nachteile geltend machen können.

Konkret würde dies beispielsweise für den derzeit im Handel geplanten Einsatz von RFID auf Objektebene bedeuten, dass

- RFID-Chips am Ladenausgang als Bestandteil des Bezahlvorgangs unbrauchbar gemacht werden oder mit einer anderen, ähnlich effektiven Schutzfunktion (z.B. Passwort- oder PIN) gegen ein unautorisiertes Auslesen versehen werden;
- der Kunde die Möglichkeit hat, die Chipfunktionalität auf seinen expliziten Wunsch hin im Produkt zu belassen;
- der Kunde die Möglichkeit hat, trotz unbrauchbar gemachter RFIDs Waren noch umzutauschen oder auf Garantieleistungen zurückzugreifen, wenn er den geforderten Nachweis (Kassenbon) beibringen kann.

Lösungen zum Schutz der informationellen Selbstbestimmung im UC müssen einfach gestaltet werden, so dass ihre Nutzung weder hohe Aufmerksamkeit noch viel Zeit erfordert. Zur Bedienung der Schnittstellen zu den Hintergrundsystemen, zur Nutzerkontrolle, zur Bestimmung der personenbezogenen Daten nach Art und Umfang sowie ihrer Verwendungszwecke bedürfen UC-Systeme eines „persönlichen Identitätsmanagers“. Er soll nach den Präferenzen des Nutzers die technische Interaktion mit einem berechtigten Hintergrundsystem ermöglichen und Art und Umfang der Daten sowie ihren Verwendungszweck freigeben. Eine weitergehende Verwendung der Objektdaten zu anderen Zwecken als der Diensterbringung kann über ihre Pseudonymisierung ermöglicht werden, wenn die Identifizierungsdaten gegen einen unbefugten Zugriff ausreichend geschützt und ihre Zweckbindung gewährleistet sind. Die Alternative ist die Implementierung eines "Ausschaltknopfes", über den der Nutzer sich aus einem UC-System auskoppeln kann.

9.2 Anforderungen aus dem und an das Datenschutzrecht

Durch UC-Systeme werden sich die Verknüpfungsmöglichkeiten personenbezogener Daten signifikant erhöhen: So werden in den Systemen bzw. ihren Komponenten personenbezogene Daten aus Kunden- und Zahlungskarten, einer Videoüberwachung, der Erfassung biometrischer Informationen, den IP-Adressen vernetzter Geräte, der jeweiligen Gerätenummer, ihrem Standort bzw. dem Standort des Nutzers, Informationen über das konkrete Objekt sowie Informationen aus elektronischer Kommunikation der Systeme, Komponenten und Objekte in den Logfiles miteinander verknüpft werden. Die Brisanz liegt in der hohen Aussagekraft dieser Informationen über Nutzer bzw. Kunden und ihr konkretes Verhalten. Darüber

hinaus bergen UC-Anwendungen eine neue Qualität der Überwachbarkeit der privaten und sozialen Interaktion der Menschen untereinander mit vermutlich tiefgreifenden Konsequenzen für die individuelle Selbstentfaltung und das persönliche Selbstverständnis. Zum Schutz der informationellen Selbstbestimmung der Betroffenen bedarf es einer konsequenten Anwendung der Regelungsmechanismen des geltenden Datenschutzrechts und seiner Kontrollmechanismen.

Die Verantwortung der Betreiber von UC-Systemen für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss gestärkt werden. Wer Lesegeräte aufstellt, aus Objekten UC-Daten erhebt, speichert und in Hintergrundsystemen verarbeitet, ist gegenüber den Betroffenen für die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung, die Wahrung seiner Datenschutzrechte sowie der Datensicherheit verantwortlich. Entsprechendes gilt, wenn personenbezogene Daten in den Chips der Objekte erhoben, verarbeitet oder genutzt werden. Technische Schutzmaßnahmen allein können die informationelle Selbstbestimmung im UC nicht gewährleisten.

Die Stärkung der datenschutzrechtlichen Verantwortung sollte für den Einsatz von UC-Systemen durch eine unabhängige Zertifizierung ihrer Anwendung in definierten Verantwortungsräumen erfolgen (Datenschutz-Audit), mit der gegenüber den tatsächlich und potenziell Betroffenen die Gewährleistung ihrer Datenschutzkonformität bestätigt wird. Kriterien sind die Rechtmäßigkeit des Systems, insbesondere seine Datensparsamkeit, die Einhaltung der Zweckbindung, die Transparenz der Datenverwendung, die Wahrung der Betroffenenrechte sowie die Datensicherheit. Eine solche Auditierung sollte aus Akzeptanzgründen freiwillig erfolgen.

Von zentraler Bedeutung für die Verwendung von UC-Daten aus verteilten Systemen und Komponenten ist die Entwicklung und Implementierung von Konzepten der Pseudonymisierung personenbezogener Daten. Bei entsprechender Gestaltung ermöglichen diese Konzepte eine Verwendung und Auswertung pseudonymisierter Daten, ohne das informationelle Selbstbestimmungsrecht der Betroffenen zu beeinträchtigen. Derartige Konzepte bedürfen allerdings auch einer rechtlichen Flankierung, indem die Zuordnungslisten mit den Pseudonymen und ihren Identifikatoren gesonderten vertrauenswürdigen Institutionen übergeben und besonderen Schutzregeln in Form einer strikten Zweckbindung unterworfen werden.

Die datenschutzrechtliche Verantwortung des UC-Betreibers kann durch ein Bündel von Maßnahmen auf der Grundlage des geltenden Rechts gestärkt werden:

- Die Selbstverpflichtung der Betreiber, gegenüber den tatsächlich und potenziell Betroffenen nur die UC-Daten zu erheben, zu verarbeiten und zu nutzen, die für einen konkreten und von dem Betroffenen gewünschten Dienst erforderlich sind.
- Das Verbot der Bildung von Kunden- und Nutzungsprofilen und ihre Verwendung für andere Zwecke als der Diensterbringung, es sei denn der betroffene Nutzer hat ausdrücklich eingewilligt.
- Die strikte Zweckbindung der erhobenen Daten auf die Erbringung des Dienstes.
- Die Stärkung der Mechanismen der Selbstkontrolle durch den betrieblichen Daten-

schutzbeauftragten sowie die Durchführung einer datenschutzrechtlichen Vorabkontrolle.

- Systemspezifische Best Practices-Regeln können Anwendern und Nutzern die Gewährleistung von Datenschutz und Datensicherheit erleichtern. Diese Maßnahmen bedürfen der Flankierung durch eine qualifizierte Beratung und Kontrolle durch die Aufsichtsbehörden, deren Funktionen zum Abbau des existierenden Vollzugsdefizits zu stärken sind.

Begleitend bedarf es wirksamer Instrumente, um Verstöße gegen Datenschutzbestimmungen sowie gegen Selbstverpflichtungen mit einer ausreichenden präventiven Wirkung zu sanktionieren und so das Vertrauen der Betroffenen in die Wirksamkeit des Datenschutzes zu erhalten bzw. zu stärken. Ausdrücklicher Sanktionen bedarf es insbesondere bei Verstößen gegen Transparenzpflichten, dem unberechtigten Auslesen von UC-Daten sowie bei Verstößen gegen den Grundsatz der Zweckbindung.

Analog der Figur der Verkehrssicherungspflichten trägt derjenige die Verantwortung für die Rechtmäßigkeit der Datenerhebung, -verarbeitung und –nutzung, der UC-Systeme oder Komponenten aufstellt und betreibt. Entsprechendes sollte auch für die Verantwortung für technische Fehler oder Fehlfunktionen gelten. Wegen der Unübersichtlichkeit heimlicher Datenerhebungen sollte derjenige, der Lesegeräte aufstellt oder betreibt, die Beweislast für Art und Umfang seiner Datenerhebungen tragen. Entsprechendes sollte auch für die Inhaber des Hausrechts bzw. entsprechender Verkehrssicherungspflichten gelten, die eine generelle Verpflichtung gegenüber ihren Besuchern haben, sie auf die Tatsache des Auslesens hinzuweisen und die Rechtmäßigkeit entsprechender Lesevorgänge nachzuweisen.

Neben der Lösung von Sicherheitsfragen in UC-Anwendungen bedarf es eines wirksamen vorbeugenden Schutzes vor einer virtuellen Belästigung (Spam) in oder durch UC-Anwendungen.

9.3 Förderung von Forschung und Entwicklung

Der IT-Sicherheit kommt zum Schutz der Rechte und Interessen der Anwender sowie der Nutzer und Betroffenen eine grundlegende Bedeutung für die Entwicklung von gesellschaftlichen und technischen Innovationen zu. Hierzu bedarf es einer Forschungsförderung, die sich nicht auf rein technisch orientierte Projekte beschränken, sondern einen umfassenden anwendungsorientierten Ansatz der interdisziplinären Forschung und Entwicklung verfolgt. Sie muss neben den technischen insbesondere auch ökonomische, rechtliche und soziale Aspekte einbeziehen, um wirksame Gestaltungsoptionen entwickeln und anbieten zu können.

Von zentraler Bedeutung für die Entwicklung von einerseits innovativen, aber andererseits auch von den Betroffenen akzeptierten Anwendungen des Ubiquitären Computing sind insbesondere:

- **Kryptographische Grundlagenforschung**

Sowohl allgemein als auch speziell für UC-Umgebungen ist verstärkte Forschung zu kryptographischen Algorithmen und Protokollen sowie zur Verifikation von Sicherheitseigenschaften notwendig.

Zum Schutz der Betroffenen bedarf es der Grundlagenforschung zur Gewährleistung von Anonymität und Unbeobachtbarkeit in UC-Systemen sowie ihrer technischen Umsetzbarkeit.

- **Forschung und Entwicklung von Pseudonymisierungsverfahren**

Verfahren der Pseudonymisierung bieten bei einer entsprechenden Gestaltung den idealen Kompromiss, um personenbezogene Daten, die einer strikten Zweckbindung unterliegen, auswerten zu können, ohne die Datenschutzinteressen der Betroffenen zu gefährden. Jedoch bedarf die Entwicklung derartiger Konzepte für Daten aus verteilten UC-Systemen noch erheblicher Forschungsanstrengungen. Hierzu sind technisch-organisatorische Konzepte des verteilten Wissens, ihrer statistisch-mathematischen Absicherung sowie die rechtlichen Rahmenbedingungen einschließlich der Voraussetzungen und Mechanismen einer erlaubten Reidentifizierung zu entwickeln.

- **Forschung zu rechtlichen Rahmenbedingungen**

UC-Anwendungen bedürfen wegen ihrer erheblichen Auswirkungen auf das informationelle Selbstbestimmungsrecht der Betroffenen der wirksamen rechtlichen Rahmenbedingungen, um Risiken für Datenschutz und Datensicherheit sowie einem Vertrauensverlust der Betroffenen vorzubeugen. Die geltenden datenschutzrechtlichen Regelungen sind daher regelmäßig einer unabhängigen Überprüfung und Bewertung zu unterziehen, um weitere Schutzlücken und den Bedarf für eine Nachjustierung zu identifizieren. Hierzu gehört auch die rechtstatsächliche Frage, ob und inwieweit die Betreiber von UC-Anwendungen ihrer datenschutzrechtlichen Verantwortung gegenüber den Betroffenen nachkommen. Besondere Bedeutung hat die Förderung und Entwicklung proaktiver Regelungsstrategien und -instrumente, die die Verantwortung der UC-Anwender stärkt, die Schutzrechte der von den Anwendungen Betroffenen einzuhalten. Zudem bedarf es einer gezielten Forschungsförderung, damit die erforderlichen rechtlichen Rahmenbedingungen für leistungsfähige Pseudonymisierungsverfahren entwickelt und für UC-Anwendungen bereitgestellt werden können.

- **Forschung zu sicherer Softwareentwicklung**

Aufgrund des größeren Einflusses auf das Persönlichkeitsrecht des Einzelnen und des Strukturmerkmals der Allgegenwärtigkeit muss die Fehleranfälligkeit der Software für UC-Systeme deutlich reduziert werden. Tests und Validierungen von UC-Systemen müssen höheren Anforderungen genügen, als dies heute für Anwendungen im Internet üblich ist. Sicherheit und Datenschutz müssen von Anfang an in die Systementwürfe integriert werden.

Zur Gewährleistung der Transparenz im Bereich IT-Sicherheit und der Interoperabilität von Produkten unterschiedlicher Hersteller bedarf es der gezielten öffentlichen Förderung von Open Source-Software, wie etwa die Weiterentwicklung von sichereren Betriebssystemen wie z.B. OpenBSD[742].

- **Forschung zur multilateralen Sicherheit**

Sicherheit und informationelle Selbstbestimmung sind in der elektronischen Kommunikation

[742] http://www.openbsd.org/

zwei zentrale Ziele, die teilweise auch miteinander kollidieren können. Diese Zielkonflikte stellen interessante Herausforderungen an die Forschung und eine nachfolgende praktische Umsetzung dar, die konzentrierter als bisher verfolgt werden müssen. Es bedarf insbesondere der Forschung zur Sicherheit von P2P-Systemen, um diese auch für zentrale Internetdienste verlässlich einsetzbar zu machen.

Ein wichtiger Forschungsgegenstand ist die multilaterale Sicherheit in UC-Umgebungen. Alle fortgeschrittenen Szenarien gehen von komplexen Betreibermodellen mit anbieter- und nutzerübergreifenden Workflows aus. Da die gesamte Sicherheit des Systems von allen (!) Teilkomponenten und dem Verhalten aller Beteiligten abhängt, werden hier ähnlich wie bei Internetdiensten neue Organisationsformen, Verträge und technische Konzepte zur Erreichung des benötigten Sicherheitsniveaus erforderlich.

- **Forschung zu nutzerzentriertem Identitätsmanagement**

Nutzerzentriertes Identitätsmanagement ist ein Ansatz, den Nutzern die Kontrolle über ihre Daten auch in komplexen datenverarbeitenden Umgebungen zu gewähren. Dabei fungiert ein „persönlicher Identitätsmanager" aus Nutzersicht als „Trusted Device" und benutzerkontrolliertes Interface zur UC-Umgebung. Die Forschung zum nutzerkontrollierten Identitätsmanagement[743] und „persönlichen Identitätsmanagern" steckt noch in den Anfängen. Auch fehlen noch Standards etwa bezogen auf die Kommunikationsprotokolle mit UC-Umgebungen, wie z.B. auch zum Aushandeln von Datenschutz-Policies zwischen Anbieter und Nutzer.[744]

Ein weiterer Forschungsgegenstand ist die Gestaltung der Bedienoberflächen (Human Computer Interface, HCI) auf „persönlichen Identitätsmanagern".

Von großer Bedeutung für die Gewährleistung der informationellen Selbstbestimmung ist die Weiterentwicklung von Anonymisierungssystemen wie TOR[745] und AN.ON[746], um sie in UC-Systemen einsetzen zu können.

- **Forschung zu automatisiertem Datenschutzmanagement**

Ein automatisiertes Datenschutzmanagement kann zur Anhebung des faktischen Datenschutzniveaus in UC-Anwendungen und zur Behebung des existierenden Vollzugsdefizits einen wesentlichen Beitrag leisten. Es ermöglicht automatisierte Kontrollen durch die Organisation selbst wie auch durch Aufsichtsbehörden, ob und inwieweit Datenschutzstandards eingehalten werden. Auf diese Weise können gesetzliche wie unternehmensinterne Vorgaben nicht nur stichprobenartig, sondern auch flächendeckend überprüft und sichergestellt werden. Automatisierte Prüfungen erweisen sich für Organisationen als ökonomisch und für die Rechte der Betroffenen als effektiv, weil sie eine höhere Anwendungstreue, aber auch eine erhöhte Personaleffizienz ermöglichen. Für UC-Systeme kann über ein automatisiertes

[743] Siehe u.a. http://www.prime-project.eu/

[744] Aufgebaut werden kann hier z.B. auf das P3P-Protokoll des W3C, http://w3.org/p3p/

[745] http://tor.eff.org/

[746] http://www.anon-online.de/

Datenschutzmanagement eine realistische Kontrolldichte datenschutzrechtlicher Vorgaben gewährleistet werden, die allein über die Mechanismen der Selbstkontrolle sowie der „manuellen“ staatlichen Datenschutzaufsicht nicht möglich ist.

Forschungsbedarf besteht zur Identifizierung und Standardisierung der einschlägigen Indikatoren für UC-Anwendungen, nach denen Datenschutzmanagementsysteme rechtskonform automatisiert ihre Prüfungen durchführen können.

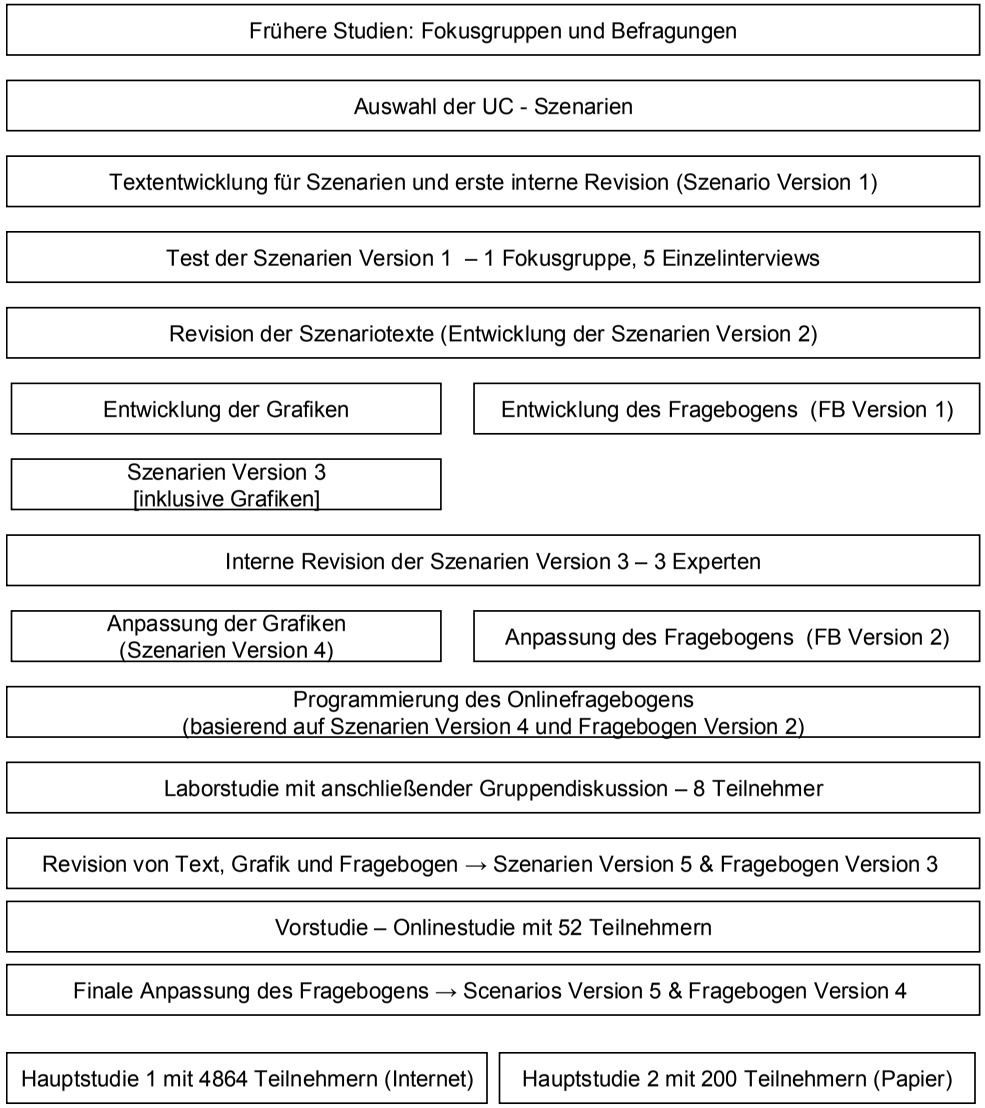
- **Usability-Forschung zur Entwicklung von einfachen Datenschutzschnittstellen**

Zur Verwaltung der eigenen elektronischen Identitäten und zur unmittelbaren Reaktion auf die Umgebung bedarf es komfortabler Schnittstellen, die von den Nutzern ohne größere Zeitinvestitionen und ohne Lernaufwand bedient werden können. Eine der Kernfragen ist die Abbildung und Übersetzung von Handlungsoptionen. So kann eine Datenübermittlung dadurch unterbunden werden, indem der Nutzer eine Antenne (ggf. reversibel) abtrennt oder im wahrsten Sinne des Wortes „einen Stecker zieht“. Eine andere Aktionsform wäre, dass der Nutzer seinem „Privacy-Manager“ den Wunsch nach Anonymität dadurch mitteilt, dass er sein Gerät in eine bestimme Richtung dreht. Die beiden Beispiele zeigen, dass die Handlungsformen einerseits in Anlehnung an die Traditionen der Offline-Welt angeboten werden müssen, andererseits aber auch einer medien- und technikspezifischen Konkretisierung und Weiterentwicklung bedürfen. Eine systematische Forschung hierzu fehlt noch.

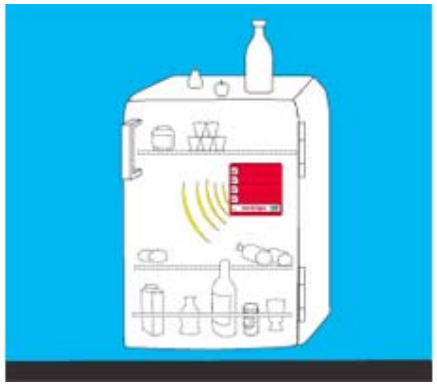
10 Appendix zu Kapitel 5

1. Beschreibung der Studiendurchführung
2. Szenario 1 der BMBF/ZEIT – Studie
3. Szenario 2 der BMBF/ZEIT – Studie
4. Szenario 3 der BMBF/ZEIT – Studie
5. Szenario 4 der BMBF/ZEIT – Studie
6. Tabelle 1: Teilnehmerstatistik
7. Tabelle 2: Beta-Gewichte (*100) der Regressionen
8. Tabelle 3: Vergleich der Bewertungen für die Kontrollvariationen sowie die Variation des Befragungsmediums
9. ANOVA der Altersunterschiede in der Nützlichkeitsbewertung
10. Tabelle 4: Korrelationen zwischen wahrgenommener Kontrolle und wahrgenommenem Privacy-Risiko

Appendix 1: Beschreibung der Studiendurchführung



Appendix 2: Szenario 1 der BMBF– Studie (durchgeführt in Kooperation mit der Wochenzeitung DIE ZEIT)



Der
intelligente
Einkaufszettel

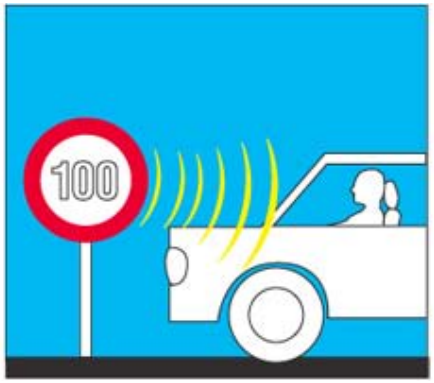
Es ist das Jahr 2015...

Es ist normal geworden, dass viele Lebensmittel des täglichen Bedarfs nicht mehr selbst im Geschäft gekauft, sondern den Haushalten angeliefert werden. Dies spart Zeit und Mühe. Die Bestellung erfolgt automatisch. Man kann alle Sachen beziehen, die man sonst im Supermarkt kaufen würde. Dazu hat fast jeder Kühlschrank einen integrierten Elektronischen Einkaufszettel, den EZ wie ihn alle nennen.

Der EZ ist ein kleiner Bildschirm, der standardmäßig auf jedem Kühlschrank angebracht ist. Er erfasst mit Sensoren, was noch in meinem Kühlschrank ist. Ist nicht mehr genug da, wird der Bedarf von ihm automatisch ermittelt und sofort nachbestellt. Auf dem EZ Bildschirm am Kühlschrank wird mir die Liste mit den von ihm bereits bestellten Produkten angezeigt.

Im EZ oder per Anruf kann ich diesen Bedarf für den nächsten Einkauf ändern. Die Bestellung geht immer automatisch an solche Läden, die ein ordentliches Preis-Leistungsverhältnis anbieten oder die ich ausgewählt habe.

Appendix 3: Szenario 2 der BMBF– Studie (durchgeführt in Kooperation mit der Wochenzeitung DIE ZEIT)



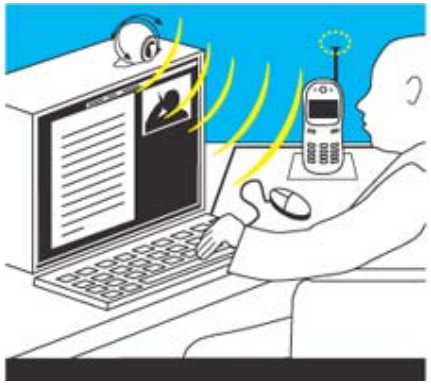
Die
automatische
Geschwindigkeitsbegrenzung

Es ist das Jahr 2015...

Mein Wagen ist aufgrund von zahlreichen Sensoren intelligent geworden. Die intelligenten Funktionen sollen das Fahren vor allem sicherer machen. Eine dieser intelligenten Funktionen ist die automatische Geschwindigkeitsbegrenzung. Diese ist bei allen Fahrzeugen außer Polizei, Feuerwehr und Krankenwagen per Gesetz vorgeschrieben.

Im Straßenverkehr funken die Tempolimitschilder am Straßenrand meinem Wagen die aktuelle Geschwindigkeitsbegrenzung zu. Fahre ich zu schnell, bremst mich mein Wagen automatisch ab. Das Navigationssystem informiert mich, dass es den Wagen aufgrund der Geschwindigkeitsbegrenzung abgebremst hat.

Appendix 4: Szenario 3 der BMBF– Studie (durchgeführt in Kooperation mit der Wochenzeitung DIE ZEIT)



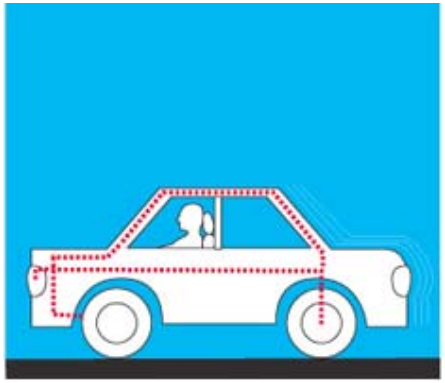
Der
intelligente
Arbeitsplatz

Es ist das Jahr 2015...

Mein intelligenter Arbeitsplatz zu Hause ist mit Rechnern, Telefon und einer kleinen Kamera (Webcam) ausgestattet. Alle Geräte sind voll automatisch miteinander vernetzt.

In den Arbeitsplatz sind viele intelligente Funktionen integriert, die mir die Arbeit erleichtern sollen. Eine Funktion des intelligenten Arbeitsplatzes ist, dass er immer automatisch bemerkt, was ich gerade tue und mich darin unterstützt. Wenn ich zum Beispiel telefoniere, schaltet er automatisch die Kamera des Bildtelefons ein und schwenkt diese optimal auf mich ein.

Appendix 5: Szenario 4 der BMBF– Studie (durchgeführt in Kooperation mit der Wochenzeitung DIE ZEIT)



Die
intelligente
Selbstwartung

Es ist das Jahr 2015...

Mein Wagen ist aufgrund von zahlreichen Sensoren intelligent geworden. Die intelligenten Funktionen sollen das Fahren vor allem sicherer machen. Eine dieser intelligenten Funktionen ist die automatische Selbstwartung der Fahrzeuge. Diese ist gesetzlich vorgeschrieben und bedeutet, dass der Wagen den Zustand seiner Teile selbständig überwacht. So wird man von Schäden nicht mehr überrascht.

Stellt das Auto fest, dass ein Teil demnächst kaputt gehen wird, weil offizielle Schadenswerte über- oder unterschritten sind, so kontaktiert es selbständig die Werkstatt und veranlasst die Bestellung des entsprechenden Ersatzteils. Ich werde darauf hingewiesen, um welches Teil es sich handelt und welches Problem besteht. Ich werde dann dazu aufgefordert, zeitnah die Werkstatt zu besuchen. Das Auto kontaktiert immer eine Werkstatt in der Umgebung mit einem akzeptablen Preis-/Leistungsverhältnis oder eine, die ich selbst als Kontakt angegeben habe.

Appendix 6: Teilnehmerstatistik

Alter			Geschlecht			Politische Einstellung			Schulabschluss			Einkommen			Fahren Sie Auto?			Besitzen Sie Auto?			Anteil des Computers an Arbeit		
	N	%		N	%		N	%		N	%		N	%		N	%		N	%		N	%
Online																							
< 20	486	10,2	weiblich	928	19,5	ganz links	96	2,0	kein Abschluss	41	,9	k. A.	1237	26,1	ja	3071	64,8	ja	2758	58,2	gar keinen / kaum	274	5,8
20-29	1676	35,3	männlich	3805	80,1	2	413	8,7	Hauptschule	62	1,3	unter 1000	1043	22,0	nein	1632	34,4	nein	1928	40,7	geringen Anteil	407	8,6
30-39	1173	24,7				eher links	1763	37,1	Realschule	379	8,0	1001 - 2000	910	19,2							etwa die Hälfte	851	17,9
40-49	780	16,4				4	871	18,3	Abitur	1634	34,4	2001 - 3000	770	16,2							überwiegenden Teil	1506	31,8
50-59	377	7,9				mitte	792	16,7	Hochschule	2605	54,9	3001 - 4000	408	8,6							fast ausschließlich	1703	35,9
> 60	252	5,3				6	434	9,1				4001 - 5000	180	3,8									
						eher rechts	306	6,4				5001 - 6000	77	1,6									
						8	37	,8				über 6000	119	2,5									
						ganz rechts	12	,3															
Total	4744	100,0	Total	4752	100,0	Total	4752	100,0	Total	4744	100,0	Total	4744	100,0	Total	4741	100,0	Total	4741	100,0	Total	4741	100,0
Papier																							
< 20	9	4,5	weiblich	102	51,0	ganz links	3	1,5	kein Abschluss	1	,5	k. A.	41	20,5	ja	136	68,0	ja	136	68,0	gar keinen / kaum	31	15,5
20-29	40	20,0	männlich	98	49,0	2	7	3,5	Hauptschule	59	29,5	unter 1000	43	21,5	nein	62	31,0	nein	62	31,0	geringen Anteil	46	23,0
30-39	40	20,0				eher links	65	32,5	Realschule	53	26,5	1001 - 2000	62	31,0							etwa die Hälfte	33	16,5
40-49	57	28,5				4	23	11,5	Abitur	35	17,5	2001 - 3000	29	14,5							überwiegenden Teil	43	21,5
50-59	53	26,5				mitte	61	30,5	Hochschule	50	25,0	3001 - 4000	16	8,0							fast ausschließlich	32	16,0
> 60	1	,5				6	12	6,0				4001 - 5000	7	3,5							6	15	7,5
						eher rechts	23	11,5				5001 - 6000	2	1,0									
						8	2	1,0													Total	200	100,0
						ganz rechts	4	2,0															
Total	200	100,0	Total	200	100,0	Total	200	100,0	Total	200	100,0	Total	200	100,0	Total	200	100,0	Total	200	100,0			

Apppendix 7: Beta-Gewichte (*100) der Regressionen

(K= Kühlschrank; A=Arbeitsplatz; T=Tempolimit; W=Wartung; M=Mean/Durchschnitt der Beta-Gewichte über alle Szenarien; o=Onlinestichprobe; p= Papierstichprobe)
Beispiel: Kontrollbilanz (links) wirkt in der Onlinestichprobe (o) auf die Nützlichkeit mit einem ß=0,05 (*100=5)

Kriterium		***Nützlichkeit***					***Einfachheit***					***Affektive Einstellung***					***Kaufintention***			***Nutzungsintention***				
		K	**A**	**T**	**W**	**M**	**K**	**A**	**T**	**W**	**M**	**K**	**A**	**T**	**W**	**M**	**K**	**A**	**M**	**K**	**A**	**T**	**W**	**M**
Kontrollbilanz	o	5	8	14	8	**9**	3	5	0	-5	**1**	12	19	29	19	**20**	6	10	**8**	7	9	15	11	**11**
Kontrollbilanz	p	7	18	12	8	**11**	-6	-11	2	-5	**-5**	6	31	26	12	**19**	14	9	**12**	0	8	22	5	**9**
Gesamtrisiko	o	5	-2	-1	5	**2**	1	4	-5	1	**1**	-7	-10	-2	-6	**-6**	-5	-3	**-4**	-5	-2	1	-1	**-2**
Gesamtrisiko	p	-9	-1	-2	-2	**-3**	11	-3	2	-8	**1**	-2	9	-6	-1	**0**	-18	3	**-7**	-13	3	-8	-2	**-5**
Funktionales R.	o	2	5	2	1	**3**	-17	-21	-15	-14	**-17**	2	3	1	3	**3**	1	0	**1**	3	-1	1	1	**1**
Funktionales R.	p	7	6	5	0	**5**	-20	-14	-18	-27	**-20**	-11	-3	0	-4	**-5**	6	-2	**2**	5	6	-2	13	**5**
Privacy-R.	o	3	4	0	2	**2**	-2	2	0	-1	**0**	-6	-11	-9	-6	**-8**	-1	0	**-1**	2	3	-5	-2	**-1**
Privacy-R.	p	7	4	-9	-8	**-1**	-1	4	15	6	**6**	-9	-13	2	-8	**-7**	4	-2	**1**	0	1	4	-9	**-1**
Psychologisches R.	o	-20	-22	-14	-14	**-18**	5	9	-2	-1	**3**	-21	-15	-9	-9	**-14**	-20	-21	**-21**	-18	-20	-17	-13	**-17**
Psychologisches R.	p	-31	-13	7	-2	**-10**	7	-8	-12	-14	**-7**	-14	-20	-23	-12	**-17**	-30	-22	**-26**	-24	-17	-10	-7	**-14**
Zeitliches R.	o	-15	-12	-3	-6	**-9**	-21	-18	-5	-15	**-15**	3	4	-2	-5	**0**	5	2	**3**	1	2	-1	1	**1**
Zeitliches R.	p	-16	-12	-4	4	**-7**	-7	-12	-3	-6	**-7**	16	11	-1	-7	**5**	-3	4	**0**	3	-9	-6	5	**-2**
Finanzielles R.	o	-1	-4	0	-1	**-2**	0	-3	-9	4	**-2**	-1	1	0	-1	**0**	-3	-1	**-2**	1	-4	-2	-3	**-2**
Finanzielles R.	p	8	0	1	-8	**0**	-7	-4	-15	5	**-5**	-2	-4	-8	7	**-2**	7	-5	**1**	-4	2	-7	-1	**-2**
Selbstwirksamkeit	o	-19	-14	-19	-21	**-18**	6	3	-4	1	**1**	-4	-1	-2	-3	**-2**	-7	-4	**-5**	-8	-6	-7	-4	**-6**
Selbstwirksamkeit	p	-9	-31	-16	-10	**-16**	-4	24	-8	15	**7**	-12	-2	-6	-4	**-6**	3	-3	**0**	0	-11	-4	-2	**-4**
Intrinsische Motivation	o	-1	1	1	1	**1**	3	5	7	3	**5**	-4	4	-7	2	**-1**	0	2	**1**	1	2	-2	-1	**0**
Intrinsische Motivation	p	-8	-6	3	-3	**-3**	2	4	6	-4	**2**	-2	5	-7	2	**0**	0	10	**5**	2	2	-2	-2	**0**
Technologische KÜ	o	-1	2	-1	3	**1**	24	22	22	26	**23**	7	6	0	0	**3**	3	2	**2**	4	7	3	6	**5**
Technologische KÜ	p	4	-2	-6	1	**-1**	32	28	33	37	**33**	12	6	0	-6	**3**	2	-5	**-1**	0	11	1	8	**5**
Vertrauen	o	6	8	7	13	**8**	14	19	18	17	**17**	8	2	4	10	**6**	9	4	**7**	9	6	2	6	**6**
Vertrauen	p	1	3	13	18	**9**	22	23	21	20	**21**	25	3	1	10	**10**	6	-4	**1**	13	11	4	22	**13**
Affektive Einstellung	o	39	35	40	37	**38**	-1	3	0	3	**1**						28	22	**25**	26	17	27	30	**25**
Affektive Einstellung	p	34	26	49	42	**38**	-31	0	-9	-4	**-11**						37	23	**30**	29	0	25	15	**17**
Nützlichkeit	o						9	4	2	13	**7**	40	36	37	38	**38**	26	35	**30**	27	37	24	28	**29**
Nützlichkeit	p						36	32	9	13	**23**	35	31	39	46	**38**	12	33	**22**	22	47	22	44	**34**
Einfachheit der Nutzung	o	4	2	1	7	**4**						-1	2	0	2	**1**	-2	1	**-1**	-2	0	4	5	**2**
Einfachheit der Nutzung	p	20	20	6	9	**14**						-17	0	-4	-3	**-6**	6	16	**11**	5	1	5	10	**5**

Appendix 8: Vergleich der Bewertungen der Szenarien für die Kontrollvariationen sowie die Variation des Befragungsmediums

(loCtrl = Variation, in der der Nutzer niedrige Kontrolle über den Dienst hat, da dieser stark automatisiert abläuft;
hiCtrl = Variation, in der der Nutzer eine relativ höhere Kontrolle über den Dienst hat, da er Aktivitäten autorisieren muss)

		Nützlichkeit			Einfachheit			Nutzungsintention			Kaufintention			Affektive Einstellung		
		loCtrl	hiCtrl	diff	loCtrl	hiCtrl	diff	loCtrl	hiCtrl	diff	loCtrl	hiCtrl	diff	loCtrl	hiCtrl	diff
Kühlschrank	online	3,22	3,37	0,15	4,01	4,07	0,06	3,02	3,14	0,12	2,74	2,89	0,15	5,11	5,39	0,29
	papier	3,50	3,66	0,17	4,01	3,96	-0,05	3,25	3,09	-0,17	3,05	3,05	0,00	5,24	5,08	-0,16
Arbeitsplatz	online	3,11	3,15	0,03	3,54	3,50	-0,04	3,20	3,23	0,04	2,58	2,68	0,10	4,48	4,75	0,27
	papier	3,35	3,39	0,03	3,40	3,51	0,11	3,32	3,19	-0,12	2,72	2,71	-0,01	4,65	4,80	0,15
Tempolimit	online	2,71	2,75	0,04	4,37	4,35	-0,01	3,20	3,31	0,11				4,65	5,00	0,35
	papier	2,73	3,10	0,37	4,15	4,38	0,23	3,55	3,77	0,22				5,12	5,68	0,56
Wartung	online	3,53	3,68	0,15	3,96	4,03	0,07	3,46	3,64	0,19				5,53	5,92	0,39
	papier	3,64	4,11	0,47	3,86	4,03	0,16	3,61	3,93	0,32				5,96	6,72	0,76
Mittelwert				0,18			0,07			0,09			0,06			0,33

		Risikofacetten																				
		Vertrauen			Funktionales~			Privacy~			Psychologisches~			Zeitliches ~			Finanzielles ~			Gesamt~		
		loCtrl	*hiCtrl*	*diff*	*loCtrl*	*hiCtrl*	*diff*	*loCtrl*	*hiCtrl*	*diff*	*loCtrl*	*hiCtrl*	*diff*	*loCtrl*	*hiCtrl*	*diff*	*loCtrl*	*hiCtrl*	*diff*	*loCtrl*	*hiCtrl*	*diff*
Kühlschrank	online	2,60	2,69	0,09	2,75	2,65	-0,10	3,52	3,44	-0,08	3,08	2,86	-0,22	2,32	2,17	-0,14	3,55	3,41	-0,14	2,83	2,67	-0,16
	papier	2,91	3,08	0,17	2,80	2,95	0,15	2,82	3,10	0,27	2,96	2,83	-0,13	2,02	1,84	-0,18	3,28	3,28	0,00	2,65	2,86	0,21
Arbeitsplatz	online	2,57	2,57	0,00	3,09	3,19	0,09	3,98	3,89	-0,10	3,24	3,10	-0,14	2,83	2,93	0,10	2,94	2,99	0,06	3,34	3,26	-0,08
	papier	2,98	2,95	-0,03	2,79	2,83	0,04	3,79	3,55	-0,24	3,24	3,14	-0,10	2,32	2,26	-0,06	3,16	3,23	0,07	3,16	3,19	0,04
Tempolimit	online	3,07	3,22	0,14	2,88	2,79	-0,09	2,96	2,91	-0,04	2,89	2,72	-0,17	2,78	2,57	-0,21	2,36	2,37	0,01	2,76	2,59	-0,17
	papier	3,21	3,57	0,36	2,73	2,66	-0,07	2,82	2,55	-0,27	2,77	2,52	-0,25	2,57	2,27	-0,30	2,61	2,59	-0,03	2,77	2,41	-0,36
Wartung	online	2,73	2,80	0,07	3,30	3,20	-0,10	2,91	2,69	-0,22	2,73	2,42	-0,31	2,52	2,33	-0,19	3,82	3,66	-0,16	3,01	2,79	-0,22
	papier	2,97	3,54	0,57	2,96	2,87	-0,08	2,70	2,21	-0,49	2,71	2,35	-0,36	2,33	1,98	-0,35	3,47	3,26	-0,21	2,84	2,56	-0,29

Mittelwert	0,17	-0,02	-0,15	-0,21	-0,17	-0,05	-0,13

Appendix 9

Tabelle 91 – ANOVA der Altersunterschiede in den Nützlichkeitsbewertungen

	ANOVA			Polynomial				Levene	Welch Robust F			
				linear		quadratic						
	F	Sig	η2	F	Sig	F	Sig	sig.	F	df1	df2	sig.
Kühlschrank	31,62	0,00	0,03	101,33	0,00	22,15	0,00	0,00	30,93	5,00	1319,47	0,00
Arbeitsplatz	12,87	0,00	0,02	16,62	0,00	21,29	0,00	0,03	12,93	5,00	981,59	0,00
Tempolimit	41,53	0,00	0,04	116,59	0,00	70,05	0,00	0,00	41,28	5,00	1329,57	0,00
Wartung	9,43	0,00	0,01	13,51	0,00	18,42	0,00	0,00	9,25	5,00	977,38	0,00

ANOVA = Statistiken der univariaten Varianzanalyse je Szenario (F-Wert, Signifikanz des F-Wertes, Effektstärke)
Polynomial = Trendtests auf lineare und quadratische Trends zwischen den Gruppen
Levene = Levene-Test auf Varianzhomogenität (wenn sig. ➔ Varianzheterogenität)
Welch Robust F = robustes F für den Fall heterogener Varianzen

Tabelle 91 – ANOVA der Altersunterschiede in den Nützlichkeitsbewertungen

	ANOVA			Polynomial				Levene	Welch Robust F			
				linear		quadratic						
	F	Sig	η2	F	Sig	F	Sig	sig.	F	df1	df2	sig.
Kühlschrank	31,62	0,00	0,03	101,33	0,00	22,15	0,00	0,00	30,93	5,00	1319,47	0,00
Arbeitsplatz	12,87	0,00	0,02	16,62	0,00	21,29	0,00	0,03	12,93	5,00	981,59	0,00
Tempolimit	41,53	0,00	0,04	116,59	0,00	70,05	0,00	0,00	41,28	5,00	1329,57	0,00
Wartung	9,43	0,00	0,01	13,51	0,00	18,42	0,00	0,00	9,25	5,00	977,38	0,00

ANOVA = Statistiken der univariaten Varianzanalyse je Szenario (F-Wert, Signifikanz des F-Wertes, Effektstärke)
Polynomial = Trendtests auf lineare und quadratische Trends zwischen den Gruppen
Levene = Levene-Test auf Varianzhomogenität (wenn sig. ➔ Varianzheterogenität)
Welch Robust F = robustes F für den Fall heterogener Varianzen

Appendix 19: Korrelationen zwischen wahrgenommener Kontrolle und wahrgenommenem Privacy-Risiko

Correlations

		szen1 kontrolle 1	szen1 kontrolle 2	szen2 kontrolle 1	szen2 kontrolle 2	szen3 kontrolle 1	szen3 kontrolle 2	szen4 kontrolle 1	szen4 kontrolle 2	elektronischer Einkaufszettel	intelligenter Arbeitsplatz	automatische Geschwindigkeitsbegrenzung	intelligente Selbstwartung
szen1 kontrolle 1	Pearson Correlation	1	,754**	,347**	,351**	,213**	,202**	,340**	,342**	,514**	,266**	,127**	,261**
	Sig. (2-tailed)		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	5061	5061	3983	3983	5060	5059	3996	3996	5061	3984	5061	3997
szen1 kontrolle 2	Pearson Correlation	,754**	1	,327**	,357**	,222**	,247**	,332**	,364**	,522**	,258**	,168**	,292**
	Sig. (2-tailed)	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	5061	5061	3983	3983	5060	5059	3996	3996	5061	3984	5061	3997
szen2 kontrolle 1	Pearson Correlation	,347**	,327**	1	,791**	,228**	,190**	,305**	,295**	,270**	,548**	,160**	,207**
	Sig. (2-tailed)	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	3983	3983	3986	3986	3985	3984	3872	3872	3986	3985	3986	3873
szen2 kontrolle 2	Pearson Correlation	,351**	,357**	,791**	1	,207**	,209**	,310**	,338**	,300**	,588**	,182**	,246**
	Sig. (2-tailed)	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000
	N	3983	3983	3986	3986	3985	3984	3872	3872	3986	3985	3986	3873
szen3 kontrolle 1	Pearson Correlation	,213**	,222**	,228**	,207**	1	,628**	,324**	,295**	,203**	,154**	,367**	,231**
	Sig. (2-tailed)	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000
	N	5060	5060	3985	3985	5063	5062	3998	3998	5063	3986	5063	3999
szen3 kontrolle 2	Pearson Correlation	,202**	,247**	,190**	,209**	,628**	1	,272**	,314**	,212**	,137**	,552**	,321**
	Sig. (2-tailed)	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000
	N	5059	5059	3984	3984	5062	5062	3997	3997	5062	3985	5062	3998
szen4 kontrolle 1	Pearson Correlation	,340**	,332**	,305**	,310**	,324**	,272**	1	,770**	,307**	,213**	,174**	,460**
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000
	N	3996	3996	3872	3872	3998	3997	3999	3999	3999	3873	3999	3999
szen4 kontrolle 2	Pearson Correlation	,342**	,364**	,295**	,338**	,295**	,314**	,770**	1	,332**	,228**	,226**	,521**
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000
	N	3996	3996	3872	3872	3998	3997	3999	3999	3999	3873	3999	3999
elektronischer Einkaufszettel	Pearson Correlation	,514**	,522**	,270**	,300**	,203**	,212**	,307**	,332**	1	,350**	,223**	,384**
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000
	N	5061	5061	3986	3986	5063	5062	3999	3999	5064	3987	5064	4000
intelligenter Arbeitsplatz	Pearson Correlation	,266**	,258**	,548**	,588**	,154**	,137**	,213**	,228**	,350**	1	,193**	,206**
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000
	N	3984	3984	3985	3985	3986	3985	3873	3873	3987	3987	3987	3874
automatische Geschwindigkeitsbegrenzung	Pearson Correlation	,127**	,168**	,160**	,182**	,367**	,552**	,174**	,226**	,223**	,193**	1	,504**
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000
	N	5061	5061	3986	3986	5063	5062	3999	3999	5064	3987	5064	4000
intelligente Selbstwartung	Pearson Correlation	,261**	,292**	,207**	,246**	,231**	,321**	,460**	,521**	,384**	,206**	,504**	1
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	
	N	3997	3997	3873	3873	3999	3998	3999	3999	4000	3874	4000	4000

**. Correlation is significant at the 0.01 level (2-tailed).