

Privacy as default.
Privacy by default!

**Konzept für Privatsphäre im Ubiquitous Computing
Diplomhauptthema Lutz Schmitt – KISD 2006**

Privacy as default. Privacy by default!

KONZEPT FÜR PRIVATSPHÄRE IM UBIQUITOUS COMPUTING

DIE **DIPLOMARBEIT** VON **LUTZ SCHMITT** (WWW.LUTZSCHMITT.COM)

IN DEN LEHRGEBIETEN

INTERFACE DESIGN (IF) UND DESIGN KONZEPTE (DK)

PROF. HEIDKAMP (IF) & PROF. TUMMINELLI (DK)

AN DER **KÖLN INTERNATIONAL SCHOOL OF DESIGN** (WWW.KISD.DE)

JUNI 2006

HINWEIS ZUM COPYRIGHT

Die hier vorliegende Fassung der Arbeit ist Version 1.0 und ist unter einem **Creative Commons Namensnennung-NichtKommerziell-Weitergabe unter gleichen Bedingungen 2.0 Germany** Lizenzvertrag lizenziert.

Um die Lizenz anzusehen, gehen Sie bitte zu <http://creativecommons.org/licenses/by-nc-sa/2.0/de/> oder schicken Sie einen Brief an Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.



VERSIONSHISTORIE

V1.0 – 2006-07-14

- Neues Cover
- Ergänzung um »Vorwort der publizierten Ausgabe«
- Ergänzung um »Kapitel IV 9.3«
- Ergänzung um einige Grafiken
- Kleinere Textkorrekturen

V1.0PR – 2006-06-21

- Prüfungsversion (KISD intern)



Danksagung

Mein großer Dank geht an Monika und Ottmar Schmitt
für großartige Unterstützung im Allgemeinen und dem Finden
von Fehlern im Speziellen.

Vorwort zur öffentlichen Version 8

Vorwort 11

I. Einleitung

- 1 ÜBER DEN TITEL 14
- 2 ÜBER DIE FORM DIESER ARBEIT 14
- 3 DIE FÜNFTE DIMENSION 16
- 4 HINTER ALLEM VERBIRGT SICH KOMMUNIKATION 17
- 5 VOM INTERFACE DESIGN ZUM PROZESSDESIGN 18
- 6 THE DIGITAL DIVIDE 19
- 7 VERTRAUEN 21
- 8 DAS MISSVERSTÄNDNIS VON DER NOTWENDIGKEIT VON PRIVATSPHÄRE 22
- 9 PRIVATSPHÄRE KANN NUR DURCH MENSCHEN VERLETZT WERDEN 24
- 10 DIE VIERTE MACHT IM STAAT 25

II. Technologien

- 1 ÜBERSICHT DER NETZWERKEBENEN UND -BEZEICHNUNGEN 28
- 2 GROSSRÄUMIGE INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIEN 29
- 3 WIRELESS PERSONAL AREA NETWORK & NEAR FIELD COMMUNICATION 45
- 4 RFID 49
- 5 FÜNF-JAHRES-PROGNOSE 59

III. Umgang mit Technologien

- 1 DIE PRINZIPIELLE UNSICHERHEIT VON TECHNOLOGIE 62
- 2 DAS ENDE DER LOKALEN DATEN 63
- 3 DIE UNMÖGLICHKEIT VON FUNKTIONIERENDEM DIGITAL RIGHTS MANAGEMENT 66
- 4 TRANSPARENZ 68
- 5 ANONYMITÄT, DATENSCHUTZ UND INTERNET 70
- 6 PRIVATSPHÄRE IN ZWEI RICHTUNGEN 72

IV. Richtlinien für den Umgang mit Technologien

- 1 FAIR INFORMATION PRACTICE 76
- 2 TOWARDS A CULTURE OF SECURITY 78
- 3 RICHTLINIEN FÜR UBIQUITÄRE TECHNOLOGIEN 82

V. Das Privatsphärenmodell

- 1 GRUNDLAGEN UND REGELN 84
- 2 IDENTITÄTEN 89
- 3 SCHICHTEN DES PRIVATSPHÄRENMODELLS 94
- 4 DIENSTKLASSEN 96
- 5 GRUPPIERUNGEN UND ABHÄNGIGKEITEN 98
- 6 ZUSÄTZLICHE FILTER UND KONTROLLMÖGLICHKEITEN 100
- 7 PRIVATSPHÄRE WÄHREND DER KOMMUNIKATION 102
- 8 SCHWACHSTELLEN 105
- 9 BEISPIELE & SZENARIEN 108

Nachwort 114

Anhang

- GLOSSAR 116
- LITERATURLISTE (GEDRUCKTE PUBLIKATIONEN) 130
- LITERATURLISTE (ÖFFENTLICH ZUGÄNGLICHE EBOOKS) 132
- INTERNETQUELLEN 136

Vorwort zur öffentlichen Version

Dieses Buch ist die Diplomarbeit eines Designers und nicht eines Informatikers oder Ingenieurs. Dementsprechend endet die Betrachtung von Technologien und der darauf aufbauenden Anwendungen an der Grenze zur konkreten Umsetzung. Das hier vorgeschlagene Konzept liefert keine Bauanleitung oder Quellcode – es ist vielmehr als Privacy Framework zu verstehen, dessen Regeln und Zusammenhänge bei der Implementation von Technologien beachtet werden sollte.

Sollte, wenn Privatsphäre als wichtiges Grundrecht verstanden wird. Ob und wie Privatsphäre verstanden wird, muss diskutiert werden. Und zwar nicht nur von den üblichen Verdächtigen, wie Datenschützern, sondern auch von denen die Anwendungen und Technologien realisieren. Dazu gehören auch Designer. Da unter Designern noch wenig bis gar keine Diskussion über Privatsphäre stattfindet, sind Designer auch das primäre Zielpublikum für dieses Buch. Aus diesem Zielpublikum leiten sich auch Teile des Inhalts ab – einiges ist für Spezialisten eher zum Grundlagenwissen zu zählen und somit bereits bekannt, aber dieses Buch richtet sich eben nicht ausschließlich an Spezialisten, sondern an Generalisten, die eher den systemischen Blick auf ein sehr komplexes Thema benötigen.

Diejenigen die sich mit Privatsphäre und Datenschutz schon beschäftigen, werden vieles gegen mein Konzept einzuwenden haben. Einige Bedingungen laufen den heutigen Ansichten zum Datenschutz durchaus zuwider oder können als utopisch bewertet werden. Dies ist durchaus gewollt, geht es doch nicht darum den Status Quo zu erhalten, sondern neue Lösungen im Umgang mit Technologien zu finden.

Diejenigen die Technologien und Anwendungen realisieren, werden möglicherweise die Realitätsferne des Konzepts kritisieren. Zuviele Unternehmen und Institutionen müssten zusammenarbeiten, zuviele unterschiedliche Technologien und Protokolle aufeinander abgestimmt werden, zuviele existierende Anwendungen von Grund auf neu entwickelt werden, usw. Kurz, die tatsächliche Realisierung als ein großes Projekt ist schier unmöglich. Doch das ist auch nicht die Absicht. Das Ziel dieses Konzepts ist eine Diskussion über das ob und wie man Privatsphäre in Technologien integrieren könnte – und zwar als Voreinstellung. Es geht also um ein Umdenken bei der Realisierung von Anwendungen und nicht um das schaffen einer großen Privatsphären-Schutz-Anwendung.

Das Konzept ist also sehr abstrakt, lässt sich so aber auf viele Anwendungsfälle projizieren. Für einige dieser Anwendungen liegen bereits Rohkonzepte in der sprichwörtlichen Schublade. Im Rahmen dieser Diplomarbeit war dafür jedoch zu wenig Zeit und Platz. So muss dieses Buch vorerst ohne damit auskommen, wenn auch eine revidierte Fassung für eine zeitlich undefinierte Zukunft in Planung ist.

Lutz Schmitt, Köln, Juli 2006

Vorwort

Die Idee zu dieser Arbeit entstand durch ein Ärgernis. Bei einem Besuch in Zürich holte mich mein Gastgeber mit dem Auto am Flughafen ab. Leider hatte er sich nicht gemerkt, wo das Auto im Parkhaus abgestellt war, und wir suchten eine Viertelstunde lang danach. Der Gedanke kam mir, dass man doch eigentlich etwas gestalten könnte, das einem diese lästige Sucherei ersparen würde. Als es daran ging, ein Thema für die Diplomarbeit zu finden, erinnerte ich mich an den Vorfall in Zürich. Ubiquitous Computing und die allgegenwärtigen Technologien schienen genau das Richtige für dieses Problem zu sein. Schnell wurde mir jedoch klar, dass es eigentlich grober Unsinn wäre, wenn ich eine »Auto-im-Parkhaus-finden-Anwendung« gestalten würde, die für sich alleine stände. Eigentlich müsste man das Gesamtsystem von Verkehr in einer Stadt betrachten, und zwar alle Verkehrsmittel, -wege und -teilnehmer. Noch ein elektronisches Gadget mehr konnte nicht die Antwort sein. Ein System, das ein Auto auffinden kann, muss genauso das ganze Verkehrssystem abbilden können, wie auch das Auto und die Person ein Teil des Gesamtsystems sind. Damit zufrieden, ein spannendes Thema gefunden zu haben, reichte ich es unter dem passenden Titel ein: »Interaction Design im Stadtverkehr«.

Die ersten Recherchen zeigten, dass mein systemischer Ansatz sehr richtig war. Viele Einzelanwendungen sind in der Erprobung oder bereits in der Anwendung, und noch viel mehr sollen in den nächsten Jahren folgen. Wundervolle Ideen, die gesamte Realität mit einem dichten Kommunikationsnetzwerk auszustatten – dem Internet der Dinge. Automatisierte Kommunikationsprozesse, die uns das Leben leichter machen, die uns jederzeit und überall als mannigfaltige Dienste zur Verfügung stehen und dabei wie selbstverständlich mit der Umwelt verschmelzen. Eigentlich musste ich nur noch eine Topologie der Dienste und Technologien erstellen, und daraus ein Konzept für ein einheitliches Zugriffs- und Anwendungssystem herausfiltern und dann noch ein paar Szenarios entwerfen, um den Nutzen zu skizzieren – und Fertig. Das war zumindest die Idee.

Um nicht eine unscharfe Vision für eine mögliche Zukunft irgendwann zu skizzieren, sondern ein Konzept für eine mögliche Anwendung in der Gegenwart oder höchstens einer nahen Zukunft zu entwickeln, begann ich, mich mit den verfügbaren Technologien zu beschäftigen – allen voran RFID, eine Technologie, die so vieles möglich machen soll. Zwangsläufig stieß ich auch auf die Kritik an RFID und den beabsichtigten Implementationen, und nach einer Weile konnte ich nicht anders als festzustellen, dass es eigentlich nicht zu verantworten ist, ein Konzept für Ubiquitous Computing im städtischen Raum zu schreiben, wenn die Technologien dafür ein so eklatantes Missbrauchspotential besitzen. Zu groß schienen mir die Möglichkeiten, damit die Privatsphäre des Einzelnen zu verletzen oder gar ganz aufzuheben, und zu groß die daraus resultierenden negativen Konsequenzen.

Vor einem solchen Konzept für Ubiquitous Computing im Stadtverkehr musste also erst einmal ein Vorschlag stehen, wie die Rahmenbedingungen aussehen müssten, um es überhaupt verantworten zu können, Anwendungen von Technologien zu entwerfen und ihren Einsatz zu befürworten, Technologien, die die Vision des totalen Überwachungsstaats aus »1984« harmlos aussehen lassen. Im Anschluss würde ich dann ruhigen Gewissens mein Stadtverkehrskonzept entwickeln können.

Nach und nach rückte die Auseinandersetzung mit diesem generellen Problem, wie wir in der Informationsgesellschaft überhaupt noch eine Privatsphäre haben können, in den Mittelpunkt. Am Ende ist nun genau dafür ein Vorschlag herausgekommen. Der öffentliche Raum spielt dabei immer noch eine wichtige Rolle, auch wenn er nicht mehr explizit als solcher vorkommt. Denn gerade im öffentlichen Raum, in einem höchst dynamischen System von Kommunikationsteilnehmern, ist die Frage nach der Aufrechterhaltung von Privatsphäre und ihrer Definition enorm wichtig. Zumindest für mich, sicher sogar mehr als für viele andere. Aber genau diese Wahl, wie wichtig Privatsphäre und wie umfassend sie ist, muss erhalten bleiben. Diese Einstellung ist leider überhaupt nicht selbstverständlich, und gerade Designer scheinen sich bei der Erfindung der Ubiquitous Computing-Zukunft nicht sonderlich mit dieser Frage aufzuhalten.¹

1 Zumindest habe ich bei meiner Recherche keine Beispiele dafür gefunden, dass sich Designer über die Privatsphäre Gedanken machen. Ganz besonders nicht hinsichtlich von RFID und ähnlichen UCT.

Ich bin aufgehalten worden, nicht, weil ich ubiquitäre Technologien nicht will, sondern weil ich sie will, aber mit der Freiheit zu entscheiden, wie weit sie in meine Privatsphäre eindringen.

Diese Arbeit ist ein Vorschlag, wie das funktionieren kann. Dabei soll sie nicht als Vorwurf verstanden sein, auch wenn sie oft so klingen mag. Sie ist vielmehr eine mögliche Antwort auf die Frage nach Privatsphäre, die impliziert, dass Privatsphäre als Freiheit ein wichtiges Gut ist. Sie soll anregen, darüber nachzudenken, wenn man noch keine Antwort auf diese Frage hat oder sich diese Frage noch gar nicht gestellt hat. Sie soll ein Alternativkonzept zu den Begehren von Regierungen und Unternehmen sein, die Privatsphäre des Einzelnen immer weiter zugunsten anderer Werte einzuschränken.

Lutz Schmitt, Köln, 2006.

I. Einleitung

1 ÜBER DEN TITEL

Privacy as default. Privacy by default! Der Titel ist Analyse, Kritik und Forderung zugleich. Die gegenwärtige Nutzung und Anwendung von Informations- und Kommunikationstechnologien (ICT) ist sowohl geprägt von dem Versäumnis, die Privatsphäre zu schützen, als auch geprägt von dem Versäumnis, dies auf einfache Weise zu tun – eben »Privacy as default«. Die Privatsphäre als Voreinstellung zu etablieren, als Selbstverständlichkeit, die auch gewahrt bleibt, wenn eine Person versäumt, sich darum zu kümmern, eben »Privacy by default«, ist die Absicht dieser Arbeit.

2 ÜBER DIE FORM DIESER ARBEIT

Man könnte annehmen, dass die Behandlung eines Themas, das sich um Technologie und ihre Anwendung dreht, sich auch einer Maschinenlogik – der Abfrage von Parametern und des strikten Ableitens davon – bedienen sollte, um zu einem verwertbaren Resultat zu gelangen. Tatsächlich findet eine solche Ableitung auch statt, allerdings erst im letzten Kapitel, das die Überlegungen, Beschreibungen und Analysen der vorherigen Kapitel einfängt und als Basis nutzt. Die einzelnen Kapitel samt Einleitung reflektieren aus verschiedenen Betrachtungswinkeln ein und dasselbe Thema – die Technologien der Informationsgesellschaft.

Die Einleitung enthält grundsätzliche Überlegungen über die Informationsgesellschaft und ihre Technologien und erklärt, wo dabei die Aufgaben und Verantwortungen für Designer liegen. Sie dient vor allem der Positionierung dieser Arbeit.

Das Kapitel »Technologien« enthält Beschreibungen und Analysen der gegenwärtigen und in naher Zukunft kommenden Technologien und Anwendungen. Das Kapitel schließt mit dem Versuch einer Prognose für die kommenden Jahre ab, wie sich die ICT und UCT verbreiten und genutzt werden.

Das Kapitel »Umgang mit Technologien« betrachtet einerseits generelle Probleme bei der Nutzung von Technologie, wie etwa der Unmöglichkeit einer absoluten Sicherheit, diskutiert solche Schwierigkeiten aber auch ganz konkret – wie etwa an der Frage der Transparenz, die sich als Entscheidung

zwischen Open Source und Closed Source darstellt. Dieses Kapitel ist aber eher wie eine lose Textsammlung zu lesen. Ganz ähnlich der Einleitung nur mit einem konkreten Fokus auf den Umgang und die Nutzung von Technologien.

Das dritte Kapitel enthält Richtlinien zur Nutzung von Technologien, beschreibt also auf einer abstrakten Ebene, wie die Nutzung von Technologie aussehen sollte. Die Richtlinien stellen sozusagen den Kern dieser Arbeit dar, von dem sich einerseits die in den vorherigen Kapiteln geäußerte Kritik an den bestehenden Nutzungsformen ableitet, als auch das im nächsten Kapitel folgende Konzept, wie man diese Kritikpunkte ausmerzen könnte.

Auch wenn also die Kapitel durchaus für sich alleine gelesen werden können und nicht zwingend voneinander abhängig sind, gibt ihre Anordnung dann doch einen Sinn. Beginnend mit der Feststellung des Kontextes und seiner Bewertung, folgt der Ist-Zustand und dessen Bewertung, dem wiederum nachfolgend der Soll-Zustand gegenübergestellt wird, aus dem sich dann das Konzept ableitet, wie sich der Ist-Zustand dem Soll-Zustand annähern könnte.

Hinweisen möchte ich noch auf das Stichwortverzeichnis am Ende dieser Arbeit, das sicherlich eine wertvolle Hilfe darstellt, sich in dieser Arbeit zurechtzufinden, da doch sehr viele Fachtermini und Abkürzungen verwendet werden. Neben kurzen Erläuterungen der Begriffe bietet das Stichwortverzeichnis auch Querverweise zu anderen Stichworten, sodass es helfen kann, Zusammenhänge besser zu verstehen. Die Hinweise auf die Internetquellen enthalten oft Verweise auf die Wikipedia. Dies hat drei Gründe:

1. Sie ist frei verfügbar.
2. Im Technologiebereich sind die Inhalte oftmals sehr gut und ausführlich.
3. Die Veränderlichkeit der Wikipedia ist ideal, um die raschen Veränderungen der Technologie und die Einführung neuer Technologien nachzuvollziehen und in die richtigen Kontexte zu setzen.

3 DIE FÜNFTE DIMENSION

Die Begriffe »Ubiquitous Computing« oder »Ambient Intelligence« werden bald ausgedient haben. Sie werden heute hauptsächlich gebraucht, um zu beschreiben, wie sich die Form der Technologie ändern wird. Sie dienen der Gruppierung der Technologien, die sich nahtlos in unseren Alltag integrieren und als Technologie unsichtbar werden. Ubiquitous Computing ist die Abgrenzung zu den gegenwärtigen Technologien, die sich als grobschlächtige, unzureichende und lästige Geräte manifestieren und die mehr Mühsal verursachen, als dass sie nützen.

Wenn jedoch eine Abgrenzung zu alten Technologien nicht mehr notwendig ist, weil diese durch die neuen intelligenten und unsichtbaren Technologien abgelöst sein werden, dann hat sich auch der Begriff des Ubiquitous Computing verbraucht.

Wenn das Ziel erreicht ist und die Nutzung von Technologie zu einem selbstverständlichen, allgegenwärtigen und unbemerkten Vorgang geworden ist, erweitert sie bruchlos unser Wahrnehmungskontinuum. Sie durchdringt und interagiert mit Raum und Zeit, erweitert sie um neue Möglichkeiten. Die Verortung in den vier Dimensionen wird zum untrennbaren und notwendigen Kontext für die Prozesse und Funktionen der ubiquitären Technologien. Die Technologien werden zur fünften Dimension unserer Realität.

Nicht nur, dass dieser Begriff leichter zu merken und zu schreiben ist, er bringt viel deutlicher zum Ausdruck, wie tiefgreifend sich unsere Realität verändern wird, wenn Mark Weisers¹ Vision Wirklichkeit wird.

1 Weiser, Mark: The Computer for the 21st Century, 1991

4 HINTER ALLEM VERBIRGT SICH KOMMUNIKATION

Einer der Gründe, warum in dieser Arbeit nicht eingehend über konkrete Anwendungen und ihre Manifestierung als Geräte gesprochen wird, ist die existierende Vielzahl von Konzepten, Ideen und realisierten Lösungen. Die Vision des Ubiquitous Computing und die aufkommenden Technologien wie RFID beflügeln viele Designer. Ob nun Wearables, Augmented Reality Anwendungen, persönliche Gadgets und Helferlein – die Liste ist sehr lang und wird täglich länger. Die Möglichkeiten der allgegenwärtigen Technologien werden vielfältig und experimentierfreudig ausgelotet. Aber die wenigsten Designer blicken über ihren Vorschlag hinaus. Obwohl als Teil eines riesigen Gesamtsystems gedacht, wird sich nicht die Frage gestellt, wie der Mensch damit umgehen soll, wenn ihn Hunderte solcher Einzelanwendungen umgeben, wie er noch Einfluss auf die Zusammenhänge haben soll, wie er noch Herr seiner Kommunikation sein kann.

Konzepte und Vorschläge, wie mit den einzelnen Anwendungen als Summe umgegangen wird, gibt es so gut wie gar nicht, und erst recht nicht von Designern. Doch wie soll die Technologie unsichtbar und selbstverständlich werden, wenn wir von ihr überschüttet werden, wenn es keine Regeln und Systeme gibt, um die Kommunikation auf ein gewolltes Maß einzudämmen?

Die hier erarbeiteten Richtlinien und Konzepte sollen genau diese Fragen beantworten helfen. Wesentlich ist dabei die Technologieunabhängigkeit dieser Richtlinien, und deswegen enden die Konzepte an der Grenze zur Umsetzbarkeit mit einzelnen Technologien. Sie sind generelle Rahmenbedingungen für die Kommunikation und die Erhaltung der Privatsphäre in einer Welt mit fünf Dimensionen. Die Interaktion des Gesamtsystems muss funktionieren und steuerbar bleiben, wenn die Einzelanwendung tatsächlich nutzbringend sein soll. Und deswegen ist dies auch eine designrelevante Arbeit. Es geht nicht mehr nur um eine funktionierende Infrastruktur im Hintergrund. Die Anwendungen selber bilden das Netzwerk, also müssen sie auch die Lösungen für die Kommunikation als Teil eines Netzwerks bereits beinhalten.

5 VOM INTERFACE DESIGN ZUM PROZESSEDESIGN

Die große Vision Mark Weisers, der das Verschwinden der Computer und anderer Geräte als Verkörperungen der Technologie voraussagte, birgt viele neue Herausforderungen für diejenigen, die sich mit der Schnittstelle zwischen Mensch und Technologie beschäftigen, aber auch ungeahnte Möglichkeiten. Wenn die Technologie unsichtbar wird, dann auch die Grenzen, die sie bisher der Schnittstelle zwischen Mensch und Computer auferlegt hat. Der Mensch als Benutzer und die Funktion als Nutzen treten in den Mittelpunkt. Zukünftig werden keine Interfaces mehr gestaltet, sondern Prozesse. Diese Entwicklung geht allmählich vonstatten und hat längst begonnen. In den nächsten Jahren wird sie mit Technologien wie RFID und mit im WPAN selbstständig kommunizierenden Geräten eine weitere Entwicklungsstufe erreichen. Die Vision von Mark Weiser scheint tatsächlich Realität zu werden.

Wenn es aber zukünftig hauptsächlich um Prozesse geht, dann wird eine der wesentlichen Herausforderungen sein, diese erfahrbar zu machen. Heute ist Technologie leicht erkennbar – die Formensprache der Geräte, die Art der Eingabegeräte und die Formen der Ausgabe sind auf wenige und bekannte Formen beschränkt. Die Grenzen der Technologie sind also nicht nur limitierend, sondern helfen, die Technologie zu identifizieren.

Doch Technologie wird nicht mehr wie Technologie aussehen müssen. Wie wird man zukünftig einen ePaper-Computer von einem Blatt Papier unterscheiden können? Und wie wird man erkennen können, wie er zu bedienen ist?

Noch sind viele dieser unsichtbaren Technologien bestenfalls in Forschungslabors zu finden, aber mit dem breiten Einzug von RFID-Systemen in den Alltag stellt sich die Herausforderung, Prozesse begreifbar und erfahrbar zu machen, schon heute. Dass es dringend solcher Konzepte bedarf, zeigt die große Diskussion um diese Technologie.

6 THE DIGITAL DIVIDE

Im Rahmen der Diskussion um die kommenden ICTs wird auch immer wieder von der Gefahr des Digital Divide gesprochen. Damit ist einerseits auf globaler Ebene der immer weiter auseinanderklaffende Graben zwischen Industrie- und Entwicklungsländern gemeint, der sich durch die ICTs noch verstärken könnte. Auf der einen Seite die hochtechnologische, vollvernetzte Weltgesellschaft und, davon ausgeschlossen, auf der anderen Seite die unterentwickelten Regionen, die eine solche Infrastruktur nicht besitzen. Konferenzen wie die WSIS² haben diese Thematik als zentrales Problem für die Weltgesellschaft ausgemacht.

Für diese Arbeit jedoch wichtiger ist der Digital Divide auf kleinerer Ebene. Es wird befürchtet, dass die Durchdringung des Alltags mit ICT zu einer Trennung innerhalb der Gesellschaft führt, nämlich zwischen denen, die intellektuell in der Lage sind, diese Technologien zu nutzen, und denen, die das nicht können. Schon heute gehören Computerfachkenntnisse in fast allen Arbeitsbereichen zu den Grundqualifikationen. Ohne diese Qualifikationen stehen nur noch wenige Arbeitsplätze offen. Die Beherrschung von Technologie wird so zur Hürde, um am Arbeitsleben teilzunehmen.

Von dieser Feststellung ausgehend, wird befürchtet, dass durch die Durchdringung des gesamten gesellschaftlichen Lebens mit ICT diese Hürden überall existieren werden und so eine neue soziale Unterschicht entsteht. Um dieser Gefahr entgegenzuwirken, wird seit einiger Zeit nach Lösungen gesucht, Technologiebenutzung in die schulische Ausbildung zu integrieren.

Dass es heute tatsächlich Ansätze zu einer solchen Trennung gibt, kann nicht geleugnet werden. Ebenso wenig, dass die Nutzung heutiger Technologien und Anwendungen sehr kompliziert ist und einen hohen Lernaufwand erfordert.

Tatsächlich haben sich aber die ICT auch so weit verbreiten können, weil sie mittlerweile viel einfacher zu nutzen sind. Die Interfaces sind besser und intuitiver geworden. Der Lernaufwand ist merklich gesunken. Diese Entwicklung wird sich weiter fortsetzen, bis hin eben zum unsichtbaren

2 siehe WSIS: Golden Book, 2005

Computer. Der grundlegende Ansatz des UC ist also geeignet, den Digital Divide zu minimieren. Die Herausforderung, die zukünftig auf Designer in dieser Hinsicht zukommt, wird die Möglichkeit sein, diese unsichtbare Technologie begreifbar zu gestalten. Technologie sollte nicht zu unerklärlicher Magie werden, die nur Eingeweihte begreifen und wirklich kontrollieren können. Auch wenn die klobige Technologie in Form von Geräten und Kabeln verschwindet, muss sie als Entität begreifbar sein, damit nicht das Gefühl der Ausgeliefertheit und Ohnmacht entsteht. Der alte Digital Divide, der zwischen Nutzern und Nutzungsunfähigen entstanden ist, sollte nicht durch einen Digital Divide zwischen denen, die Technologie begreifen und kontrollieren können, und denen, die ihr ohnmächtig ausgeliefert sind, ersetzt werden. Oder kurz: Jeder sollte wissen, wo der Ausschaltknopf ist, selbst wenn ihn keiner betätigen will.

7 VERTRAUEN

Immer wieder wird in der vorliegenden Arbeit von Vertrauen gesprochen werden. Dabei geht es grundsätzlich um zwei Formen des Vertrauens. Einerseits das Vertrauen in die Technologie, dass sie das tut, was sie tun soll. Nicht mehr und nicht weniger. Andererseits das Vertrauen in Menschen und Institutionen, dass sie die ihnen gegebenen Informationen und Kommunikationswege nicht gegen uns gebrauchen. Vertrauen ist die Grundlage für Kommunikation.

Während Vertrauen zwischen Menschen ein komplexer sozialer Prozess ist, in den Designer nur beschränkt helfend eingreifen können, sieht das bei den Technologien und ihren Anwendungen ganz anders aus. Prozessstrukturen, Interfaces und die Transparenz der Funktion sind wesentliche Faktoren, um Vertrauen in eine Technologie zu gewinnen. Misstrauen in Technologie verhindert eine unbeschwerte Nutzung. Wenn man Angst haben muss, dass nicht das passiert, was passieren soll, dann wird man solche Technologien gar nicht oder nur sehr argwöhnisch nutzen. Für die Vision der unsichtbaren und selbstverständlichen Technologie ist ein solches Szenario vernichtend. Eine der Hauptaufgaben, auch für Designer, in Ubiquitous Computing- Szenarien wird also sein, die Technologien und ihre Anwendungen vertrauenswürdig zu machen. Dazu gehört auch, dass die Technologie nicht nur das tut, was sie soll, sondern auch, dass sie einen größtmöglichen Schutz davor bietet, nicht gegen uns benutzt zu werden.

Designer müssen auch solche Sicherheitsmaßnahmen mit in die Anwendungskonzepte integrieren. Sie müssen dabei zur Selbstverständlichkeit werden, das heißt aber auch, dass sie einfach zu benutzen sein müssen. Eine Forderung, von der gegenwärtige ICT-Anwendungen größtenteils noch weit entfernt sind.

8 DAS MISSVERSTÄNDNIS VON DER NOTWENDIGKEIT VON PRIVATSPHÄRE

In Gesprächen über Privatsphäre und Überwachung mit Personen, die sich mit der Problematik des Datenschutzes und der informationellen Selbstbestimmung nicht eingehend beschäftigt haben, taucht oftmals ein Unverständnis über die Verbissenheit auf, mit der Datenschützer auf Einhaltung der Privatsphäre pochen. Der dogmatische Schutz der Privatsphäre scheint vielen überzogen und unangebracht. Die vorgebrachten Beispiele zur Verletzung der Privatsphäre werden gekontert mit den Vorteilen, die daraus aus der jeweiligen Verwendung der Daten erwachsen.

Solche Diskussionen, die oft in gegenseitigem Unverständnis enden, zeigen deutlich, dass jede Person andere Vorstellungen über die Wichtigkeit von Privatsphäre hat. Für den einen mag die Protokollierung aller Bewegungen auf einer Website, wie sie etwa Amazon.com vornimmt, wie eine unkontrollierbare Bespitzelung aussehen, für den anderen ist sie eine wunderbare Hilfe beim Stöbern und Entdecken unbekannter Produkte.

Privatsphäre ist also ein variabler Wert und auch die Datenschützer und Überwachungsgegner müssen akzeptieren, dass es Personen gibt, die bereitwillig ihre Privatsphäre ganz oder in Teilen aufgeben. Der grundlegende Fehler ist dabei die Wahl des Themas. Bei der Diskussion um Datenschutz und Privatsphäre muss es immer um die Wahlfreiheit gehen, um das Recht, allein gelassen zu werden, wenn man es will.³ Die Wichtigkeit der Einhaltung von Datenschutz und Privatsphäre muss jeder für sich selbst entscheiden. Aber eben diese Entscheidungsmöglichkeit muss gegeben sein.

Ein bedauerlicher Fakt ist heute, dass gerade die Kommunikationstechnologien nicht dafür ausgelegt sind, diese Wahlfreiheit zu gewährleisten, sondern, im Gegenteil, einer allgegenwärtigen Überwachung Tür und Tor öffnen. Konzeptuell gehen die heutigen ICT davon aus, dass ein Missbrauch nicht stattfindet. Aber dieser Missbrauch beziehungsweise der Entzug der Wahlfreiheit findet statt.

3 Als »the right to be left alone« wurde Privatsphäre bereits 1890 in »The Right to Privacy« von Warren und Lois D. Brandeis definiert. siehe <<http://www.louisville.edu/library/law/brandeis/privacy.html>>

Vielfach ist deswegen heute schon eine sehr absolute Wahl zu treffen: Ich nutze die Technologien und die auf ihnen basierenden Dienste und verzichte dafür auf den Schutz eines großen Teils der Privatsphäre, oder ich nutze diese Technologien nicht und erhalte so meine Privatsphäre.

Die Wahl, Technologien zu nutzen, ohne die Privatsphäre zu verletzen, besteht nicht. Diese fehlende Wahlfreiheit ist auch eine grundlegende Antriebsfeder der Verfechter einer anonymen Nutzung des Internets. Dazu mehr im Abschnitt Anonymität, Privatsphäre und ICT.

Um diese Wahlfreiheit bei der Nutzung von Technologien zu erreichen, muss eine wesentliche Richtlinie bei der Entwicklung von Anwendungen befolgt werden: »Privacy as default«. Nach heutigem Stand ist es genau umgekehrt. Ein grundsätzliches Umdenken ist also notwendig, das über kleingedruckte »Privacy Policies« hinausgeht und alle Ebenen mit einschließt, von den Technologien über die Anwendungen bis zu den Betreibern und Benutzern.

Datensammelnde Unternehmen wehren sich gegen solche Maßnahmen und tun sich schon heute schwer mit der Einhaltung der existierenden Richtlinien und Gesetze. Sie sehen teilweise durch solche Bemühungen, den Datenschutz durchzusetzen, ihr Geschäft in Gefahr. Doch die Freiheit des Einzelnen darf nicht den Geschäftsinteressen von Unternehmen untergeordnet sein. Wenn man dazu in Erwägung zieht, wie bereitwillig viele Personen heute ihre Daten offenbaren, ist die datenschutzfeindliche Haltung vieler Unternehmen noch weniger verständlich.

9 PRIVATSPHÄRE KANN NUR DURCH MENSCHEN VERLETZT WERDEN

Der Philosoph Vincent Müller stellt die These zur Debatte, dass die Privatsphäre nur durch Menschen und nicht durch Maschinen oder Computersysteme verletzt werden kann.⁴ Diese Überlegung hat einiges für sich, da die ICT eigentlich immer nur dazu dienen, eine Verknüpfung zwischen Menschen herzustellen. Ohne diese Verknüpfung, also dem Verbleiben der Informationen im Computersystem, kann eigentlich auch keine Verletzung der Privatsphäre erfolgen, denn Technologien sind nur dumme Befehlsempfänger von Menschen. Dies könnte sich jedoch ändern, wenn auch Maschinen intelligent werden und autonome Entscheidungen treffen können, die dazu geeignet sind, einen Computer als »soziales Wesen« zu klassifizieren, oder wenn automatisierte Entscheidungen dazu geeignet sind, in die Persönlichkeitsrechte eines Menschen einzugreifen.

Dieser generellen Überlegung, dass Privatsphäre nur von Menschen verletzt werden kann, stehen jedoch auch aktuelle Argumente gegenüber. Es ist bewiesen, dass alleine das Bewusstsein überwacht zu werden, ob nun ein Mensch die Überwachungsdaten auswertet oder nicht, das Verhalten von Menschen verändert. Alleine die Gegenwart von Überwachungstechnologie kann also schon als Eingriff in die Persönlichkeitsrechte und Freiheiten gesehen werden. Diese harte Linie gegenüber Technologien, die zur Überwachung geeignet sind, ist jedoch nicht haltbar, wenn man UCT nutzen will.

4 siehe <<http://www.heise.de/newsticker/meldung/69490>>. Leider war es mir nicht möglich eine Publikation über dieses Thema von Vincent Müller oder ihn selber ausfindig zu machen, um näheres zu diesen Überlegungen zu erfahren. Möglicherweise wird diese Position klarer, wenn die Dokumentation zum ZIF-Workshop »Privacy and Surveillance Technology - Intercultural and Interdisciplinary Perspectives« veröffentlicht sind. Siehe <<http://viadrina.eu.vf-fd.de/~mibpriv/workshop/>>

10 DIE VIERTE MACHT IM STAAT

Die existierenden ICT, der Ausblick auf die noch kommenden Technologien und die damit verbundenen Möglichkeiten haben dazu geführt, dass die Informationsgesellschaft ausgerufen wurde. Der Stellenwert, der diesen Technologien zugemessen wird, ist also extrem hoch. Umso wichtiger ist die Frage, wie damit umgegangen wird. Nicht alle Möglichkeiten, die sich bieten, sind ethisch vertretbar oder auch nur wünschenswert. Die Entscheidung, welcher Umgang richtig oder falsch ist beziehungsweise welcher erlaubt oder verboten ist, ist essentiell für die Informationsgesellschaft. Das Vertrauen in die Technologien benötigt nicht nur integrale Systeme, sondern auch ein Vertrauen darin, dass die Systeme im Rahmen demokratischer und ethischer Prinzipien genutzt werden. Die Richtlinien und Gesetze dafür existieren bereits teilweise, hauptsächlich als Datenschutzgesetze. Doch wer kann kontrollieren, dass diese Regeln auch eingehalten werden?

Heute ist es so, dass ein Unternehmen von einer Privatperson dazu aufgefordert werden kann, preiszugeben, welche Daten es über diese Person gespeichert hat. Vermutet die Privatperson, dass ihr nicht die volle Wahrheit gesagt wurde, kann sie sich an den zuständigen Datenschutzbeauftragten wenden. Dieser wird dann seinerseits eine Anfrage an das Unternehmen richten und eine Antwort erhalten, die er dann an die Privatperson weiterleitet. Eine Möglichkeit zu kontrollieren, ob das Unternehmen nicht auch ihm gegenüber die Unwahrheit sagt, ist nicht gegeben findet nicht statt, kann sie auch nicht. Datenschutz basiert heute also vollständig auf Vertrauen in die Einhaltung der Gesetze. Für eine Gesellschaft, deren wichtigstes Gut solche Informationen beziehungsweise Daten sind, eine unhaltbare Situation. Ein Missbrauch von Daten kann im Prinzip nicht nachgewiesen werden.

Erschwerend kommt hinzu, dass die Funktion der Datenschützer nur beratenden und beurteilenden Charakter hat. Will ein Unternehmen etwa Systeme oder Praktiken anwenden, die personenbezogene Daten betreffen, so muss ein Datenschutzbeauftragter gefragt werden, den zumindest in Deutschland jedes größere Unternehmen haben muss. Seine Beurteilung ist aber nicht bindend, sondern hat reinen Empfehlungscharakter. Wenn die Empfehlung nicht genehm ist, dann wird sie ignoriert.

Doch nicht nur im privaten Umfeld hat der Datenschutz einen schweren Stand. Immer wieder und immer öfter wird er zugunsten anderer Ziele und Bedürfnisse gelockert oder durchlöchert. Gesetze werden erlassen, die in klarem Widerspruch zur Fair Information Practice stehen, wo doch eigentlich der faire Umgang mit Informationen in der Informationsgesellschaft eine der wichtigsten Aufgaben der Gesetzgebung sein sollte. Die Infosphäre und damit die Privatsphäre hat nur eine äußerst schwache Lobby in heutigen Gesellschafts- und Staatsstrukturen.

In einer gesunden Demokratie des Informationszeitalters muss es eine Instanz geben, die die Kontrolleure und Verwalter von Informationen kontrollieren kann und niemandem verpflichtet ist außer den Informationen selbst. Deswegen kann diese Funktion nicht von Instanzen ausgeführt werden, die innerhalb der bekannten Gewaltenteilung von Legislative, Judikative oder Exekutive positioniert sind, da diese Instanzen selbst Begehrlichkeiten gegenüber den Informationen besitzen. Es braucht eine vierte Macht im Staat – die Informative⁵. Sie muss darüber entscheiden und urteilen können, ob mit Informationen gut und richtig umgegangen wird. Die Fair Information Practice muss mehr werden als eine reine Empfehlung. Sie muss Gesetz werden und auch als solches auch durchsetzbar.

So groß diese Forderung auch ist, so muss sie noch erweitert werden. Das Internet und damit die Informationen machen vor keinen Grenzen halt. Informationen haben keine Nationalität. Alle Versuche, die Rechts- und Staatenordnung auch im globalen Dorf durchzusetzen, dürfen als gescheitert betrachtet werden und werden auch niemals durchsetzbar sein. Dementsprechend müsste die vierte Macht im Staat im Prinzip global agieren können und in ihren Handlungen und Befugnissen dem Datenstrom folgen können. Unzweifelhaft wäre ein solcher Schritt mit dramatischen Veränderungen der politischen Machtverhältnisse verbunden. Staaten müssten einen erheblichen Teil ihrer Souveränität und Gewalt abgeben. Aber wenn die Weltgesellschaft wirklich von einem globalen Dorf zu einer globalen Polis werden will, wird eine solche Instanz notwendig sein.

5 Kurz nachdem ich zu dieser Forderung gekommen war, zeigte sich, dass ich nicht alleine mit einer solchen Überlegung bin. Prof. Richard de Mulder hat wohl ähnliches formuliert. Siehe < <http://www.heise.de/newsticker/meldung/72666>>. Leider war Prof. de Mulder nicht zu erreichen, um weitere Informationen zu seiner Darstellung zu erhalten.

Viele der Probleme, die heute im Zusammenhang mit dem Internet entstanden sind, sind nicht zuletzt auch der Tatsache geschuldet, dass Informationen keine Grenzen kennen, Gesetze und ihre Durchsetzung aber sehr wohl. Viele dieser Probleme werden sich erst lösen lassen, wenn eine Gleichbehandlung der Informationen stattfindet. Diese Forderung bedarf eigentlich noch weiterer Ausführungen und wirft eine Menge Fragen zur Realisierbarkeit jenseits des politischen Willens auf. Aber dass dieser ohnehin fehlt, ist angesichts der vielen Entscheidungen der letzten Jahre eindeutig, die teilweise massiv gegen die Fair Information Practice und die informationelle Selbstbestimmung verstoßen haben. Die Tendenz, die Technologien der Informationsgesellschaft auch zur Überwachung und Einschränkung von Freiheiten und der Privatsphäre zu nutzen, ist ständig spürbar.

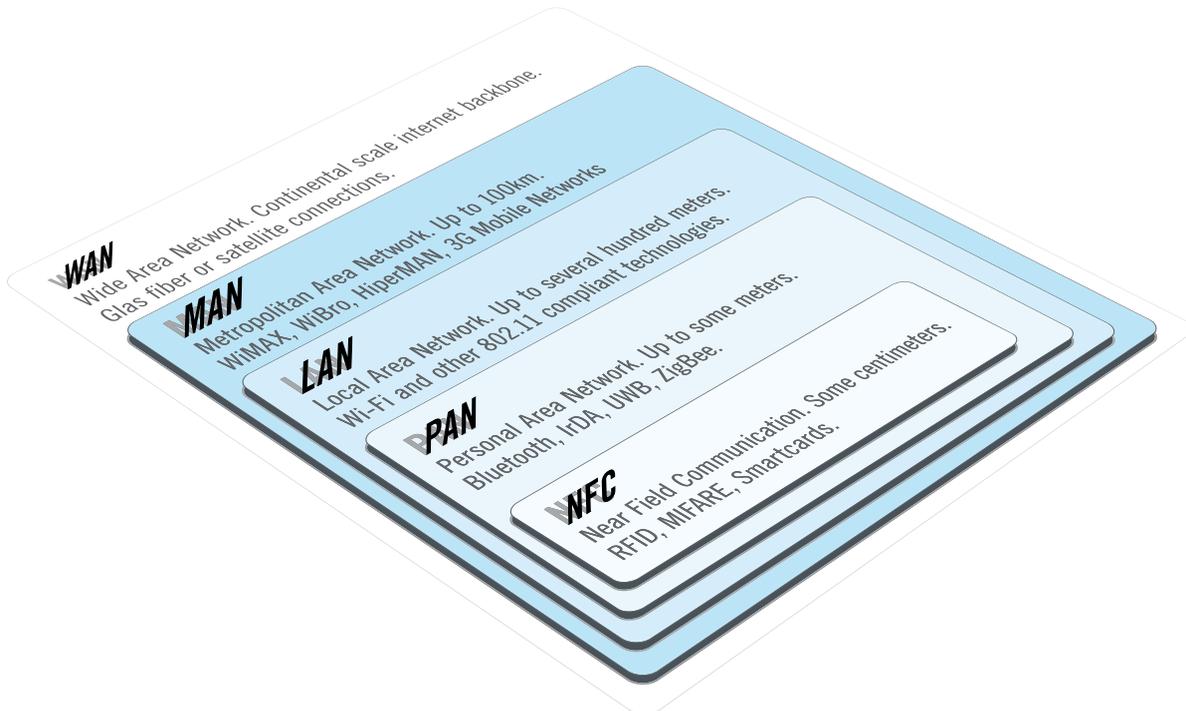
An dieser Stelle sollen weder die Notwendigkeit noch die Implikationen einer Informativ weiter besprochen werden – diese Diskussion muss an anderer Stelle fortgesetzt werden. Auch weil eine solche vierte Gewalt nicht nur Probleme lösen würde, sondern auch neue schaffen würde. Aber das Prinzip, die Kontrolleure kontrollieren zu können, damit eine Vertrauensbasis für die Informationsgesellschaft und ihre Technologien entstehen kann, ist essentiell für die Konzepte und Vorschläge dieser Arbeit. Technologie und ihre Nutzung muss kontrollierbar bleiben und Grenzen haben.

II. Technologien

ANMERKUNG

Die folgenden Erläuterungen zu den Kommunikationsnetzwerken sind an einigen Stellen stark pauschalisiert und vor allem vereinfacht. Besonders die Beschreibungen von WPAN und RFID. Dies liegt vor allem in der Tatsache begründet, dass vor allem beim WPAN die Verbreitung noch nicht allzu groß ist, und viele Technologien und Standards erst noch kommen. Die Beschreibung von RFID ist auch kurz, weil die Technologie selber im Prinzip sehr einfach ist, und weitere Ausführungen zu sehr ins technische Detail abdriften würden.

1 ÜBERSICHT DER NETZWERKEBENEN UND -BEZEICHNUNGEN



2 GROSSRÄUMIGE INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIEN

2.1 EINLEITUNG

In den letzten 15 Jahren hat sich die Kommunikationslandschaft massiv verändert. (Neben der Einführung des Internets ist dies vor allem die Mobilfunktechnologie.) Nicht nur das Internet hat diese Veränderung hervorgerufen, sondern vor allem die Mobilfunktechnologie. In Deutschland etwa gibt es pro 100 Einwohner 78,5 aktive Mobiltelefone. In anderen europäischen Ländern sieht es nicht viel anders aus. Ebenso gibt es 28 Internetanschlüsse pro 100 Einwohner.¹ Was sich wenig im Vergleich anhört, relativiert sich dadurch, dass Internetanschlüsse von mehr als einer Person genutzt werden, im Gegensatz zu Mobiltelefonen, die eher personenbezogen genutzt werden. Die Abdeckung mit Festnetztelefon- und Kabel-TV-Anschlüssen ist ebenfalls sehr hoch. Sie liegen beide in Deutschland an der 30 Millionengrenze.

Die ICT haben also auf breiter Front Einzug in den Alltag gehalten. Ebenso ist die Netzabdeckung sehr weit fortgeschritten. Fast überall in Deutschland sind die Dienste verfügbar, ob drahtgebunden oder über Funk. Sind die verschiedenen ICT zwar überall verfügbar, steht man heute jedoch vor dem Problem der fehlenden Interoperabilität. Je nachdem, was gewollt ist, muss Zugang zu einem bestimmten Netzwerk hergestellt werden. Heute hat man einen Festnetztelefonanschluss, der auch als Internetzugang dient, ein Mobiltelefon, einen TV-Kabelanschluss und so weiter und so fort. Es gibt zwar Bemühungen, diesen Wust zu vereinheitlichen, etwa durch die Kabelnetzbetreiber, die auch Internetzugang und Telefon über das Kabelnetz anbieten, oder auch durch die Festnetzanbieter, die ihrerseits in der Fernsehlandschaft mit IPTV wildern wollen. Diese sogenannten Triple-Play-Angebote haben jedoch den enormen Nachteil, dass sie alle an breitbandige und verdrahtete Anschlüsse gebunden sind. Damit endet an der Grenze zur mobilen Nutzung die Vereinheitlichung von Netzwerken und Technologien.

Bei den Mobilfunknetzwerken sollte UMTS als Mobilfunktechnologie der dritten Generation endlich auch Datendienste mit hohen Bandbreiten und somit auch hier einen vereinheitlichten Zugang zu Sprach- und

¹ Alle Zahlen über die ICT stammen sind 2003 erhoben worden.
Quelle: OECD Communications Outlook 2005.

Datendiensten erlauben. Doch wird UMTS nur zögerlich angenommen, da es für die Hauptnutzung der Mobilfunknetze, dem Telefonieren, keine besonderen Vorteile bietet und für die Nutzung als Internetzugang immer noch zu langsam und zu teuer ist. Eine maximale Übertragungsrate von 2 Mbit, wenn man alleine in einer Funkzelle ist, ist zu wenig, zumal Sprachdaten Vorrang haben und somit die Internetverbindung jederzeit auf minimalste Datenraten zusammenschrumpfen kann.

Ebenso haben die mobilen Dienste von einer unerwarteten Seite Konkurrenz bekommen – WLAN. Ende der 1990er eingeführt, passend zum Trend des mobilen Computers, hat sich WLAN erfolgreich als Technologie etablieren können. Fast kein Laptop wird heute ohne WLAN ausgeliefert, an immer mehr Orten werden Hotspots errichtet, die kostenlos oder gegen Gebühr drahtlosen Internetzugang erlauben. Doch auch wenn es immer mehr WLAN-Hotspots gibt, ein flächendeckendes Netz, wie es etwa GSM und UMTS bieten, ist mit WLAN nach IEEE 802.11 Standards nicht leicht zu errichten. Es bleibt bei punktuellen Angeboten.

Mit dem wachsenden Erfolg von VoIP-Angeboten, wie von Skype oder SIPgate, mausert sich das unkoordinierte WLAN-Netz aber dennoch zu einer ernstzunehmenden Konkurrenz für die Betreiber der anderen Mobilfunknetzwerke.

Das Angebot und die Möglichkeiten sind heute also vielzählig, und jeder Netzbetreiber und Serviceprovider schickt sich an, in den Bereichen der anderen Dienste zu wildern – ein großes Chaos, aus dem Konzepte wie Unlicensed Mobile Access (UMA) entstehen.

Das UMA-Konzept befähigt Geräte über alle Funknetze zu kommunizieren und das gerade beste auswählen zu können, und dabei dieses Roaming zwischen den verschiedenen Technologien ohne Unterbrechung einer bestehenden Verbindung zu bewerkstelligen.

Dieses Roaming zwischen den Netzen scheidet heute aber noch daran, dass für die einzelnen Netze einzelne Verträge abgeschlossen werden müssen. Roaming innerhalb einer Technologie wie GSM ist mittlerweile weithin möglich, aber fließend von GSM nach UMTS nach WLAN zu wechseln, ist bislang nur technisch möglich.

Die Idee des »Always-On« als wesentliche Bedingung von UC ist also mit den existierenden (Mobilfunk-)Netzwerken nur unzureichend realisiert. Doch der Erfolg von WLAN-Technologien wird in den nächsten Jahren die Infrastrukturgrundlage für UC in greifbare Nähe rücken lassen – in der Form von Wireless Metropolitan Networks auf Basis von WiMAX und Wi-Fi. Die Konzepte und Realisierungen dieser Funknetzwerke sind zumindest dafür geeignet. Daher werden nun im Folgenden WiMAX und Wi-Fi im Detail vorgestellt. Andere entsprechende Technologien und Standards werden nur am Rande erwähnt, nicht, weil sie die schlechtere Lösung darstellen, sondern weil sie sich konzeptuell kaum unterscheiden. Ein WiMAX- und Wi-Fi-basiertes WMAN wird hier also stellvertretend vorgestellt.

2.2 BEGRIFFSKLÄRUNGEN

WI-FI

Wireless-Fidelity oder Wi-Fi ist ein eingängiger Name für Geräte, die die Funkstandards IEEE 802.11a,b oder g unterstützen. Damit umfasst Wi-Fi alle Geräte, die heute allgemein als WLAN-Technologie bezeichnet werden. Die Standardfamilie 802.11 umfasst jedoch noch weitere Standards, die auf unterschiedlichen Protokollebenen die Kommunikation definieren. Für den allgemeinen Sprachgebrauch kann man jedoch WLAN, Wi-Fi und 802.11 synonym gebrauchen. Hier wird, der Abgrenzung zu WiMAX willen, immer von Wi-Fi die Rede sein.

Geräte nach 802.11b und g funken auf dem 2,4MHz-Band und damit auf einem Band, das fast in jedem Land lizenzfrei ist. Ein großer Vorteil, da keine regulatorischen Maßnahmen beim Einsatz befürchtet werden müssen. 802.11a ist ein weiterer wichtiger Standard, der jedoch trotz des späteren Anwendung fand. Geräte nach a funken auf dem 5MHz Band und sind damit inkompatibel zu b und g. Die Verbreitung des nachziehenden a ist auch aus diesem Grunde heute vernachlässigbar. Wi-Fi-Netzwerke sind für kleinere geographische Netzwerke mit wenigen Dutzend bis hunderten Clients gedacht. Ein Accesspoint kann mehrere Dutzend Clients verwalten und die

Sendeleistung von Wi-Fi-Geräten reicht für ein paar Meter in Gebäuden oder dutzenden Metern auf freie Sicht. Mit Sendeverstärkern und Richtantennen kann die Reichweite jedoch auch mehrere Kilometer ausgedehnt werden. Aktuell schnellste Wi-Fi-Technologie nach 802.11g kann 54Mbit Brutto übertragen. Dies ist jedoch der Idealfall. Die Übertragungsrate nimmt rapide ab bei schlechterer Verbindung oder größeren Entfernungen. Lösungen mit zwei Sendeeinheiten, um auf 108Mbit zu kommen, sind bereits auf dem Markt, aber in keinster Weise standardisiert.

Meshed Wi-Fi-Netzwerke können momentan nur über OLSR o.ä. gelöst werden. Dieses Protokoll liegt auf einer relativ hohen Ebene des OSI-Modells und verursacht dadurch einen großen Overhead. Abhilfe soll 802.11s liefern, das Meshed Networking besser implementiert. Bis dahin bleibt es bei OLSR oder anderen proprietären Lösungen.

Wi-Fi-Geräten unterstützen relativ starke Verschlüsselungsalgorithmen. Der mittlerweile in Minuten knackbare WEP-Standard ist in neueren Produkten durch WPA2 (AES) ersetzt worden. Für den AES-Algorithmus ist noch keine Lücke bekannt. Bruteforce-Angriffe auf den 256bit Schlüssel sind mit der heutigen Rechnerleistung nicht in akzeptabel schneller Zeit durchführbar.

WiMAX

Während für Wi-Fi-Netzwerke viele Accesspoints oder Repeater notwendig sind, um größere Gebiete abzudecken, ist WiMAX dafür ausgelegt, mehrere Quadratkilometer pro Funkzelle abzudecken. In der gesamten Funkzelle sollen dabei 40Mbit übertragen werden können. Aufgrund der geographischen Größe einer Funkzelle ist WiMAX auch in der Lage, mehrere hundert Clients pro Netzknoten zu verwalten. WiMAX und Wi-Fi können also als komplementäre Technologien betrachtet werden. WiMAX ist deswegen vor allem dafür gedacht, schwach besiedelte Gebiete mit Hochgeschwindigkeitsanschlüssen zu versorgen und als Wireless-Backbone in Ballungsräumen. Noch ist nicht klar, welche Frequenzen genutzt werden, Favorit scheint jedoch das 3,5Mhz-Band zu sein, das weltweit nur wenig Regulierungen unterliegt.

Die Realisierung von WiMAX-Netzwerken geschieht momentan nur zögerlich, da zwar der Standard 802.16d (fixed WiMAX) abgesegnet ist, viele jedoch 802.16e (mobile WiMAX) favorisieren, da mobile WiMAX besser bewegliche Clients und Netzknoten berücksichtigt.

WiMAX tritt nicht nur in Konkurrenz zu bestehenden drahtgebundenen Breitbandangeboten wie DSL, sondern ist aufgrund der großen Funkzellen und der damit verbundenen relativ einfachen Errichtung einer flächendeckenden Infrastruktur ein ernstzunehmender Konkurrent für GSM- und UMTS-Netze. Die notwendige Quality of Service (QoS) ist in den WiMAX-Standards bereits implementiert.

MAN/WMAN

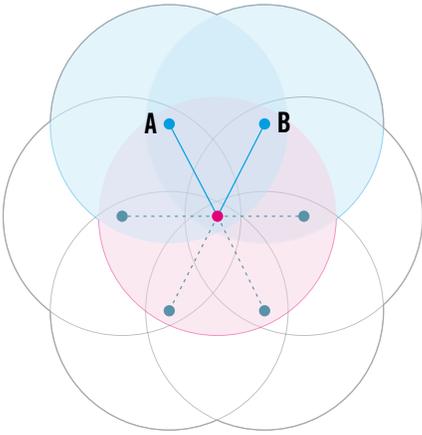
Ein Metropolitan Area Network muss zu der Infrastruktur einer Stadt gezählt werden. Im Gegensatz zu geschlossenen LANs, die ebenso lokale Hierarchien haben und bei denen kein Zugriff von nicht eingebundenen Clients möglich ist, dient ein MAN als Internetanbindung beziehungsweise Anbindung von Städten oder Regionen an ein WAN. Die Differenzierung zwischen MAN und WAN ist dabei häufig eher akademisch, da die großen TelCo-Provider sowohl WAN als auch MAN Infrastruktur anbieten. Ein MAN ist also kein geschlossenes Netzwerk, sondern ein Teil der Internetinfrastruktur. MANs werden von TelCo-Providern betrieben, in Deutschland ist dies vor allem die T-Com. Andere TelCo-Unternehmen, vor allem regional, haben aber mittlerweile eigene Netze aufgebaut. Da dies bisher hauptsächlich drahtgebunden stattfindet, ist dies mit enormen Investitionen verbunden. Einen Meter Glasfaser oder Kupferkabel zu verlegen, kostet etwa 300 Euro. Hier kommt nun das Konzept der Wireless MANs zum Tragen. Anstatt aufwändig und teuer Kabel zu verlegen, wird die Netzabdeckung mit Funknetzwerken erreicht. Durch die geringeren Investitionskosten rechnet sich so auch die Anbindung von Gebieten, wo dies mit drahtgebundenen Technologien bisher nicht rentabel war. Generell gilt, für MAN wie WMAN, dass sie vorsehen, dass ein komplettes Netz aus einer Hand entsteht. Die zukünftigen WMANs sollen sich so in jeder Hinsicht nahtlos in die jetzigen TelCo-Netzwerke einreihen beziehungsweise sie ergänzen.

2.3 NETZWERKTOPOLOGIEN & MESHED NETWORKS

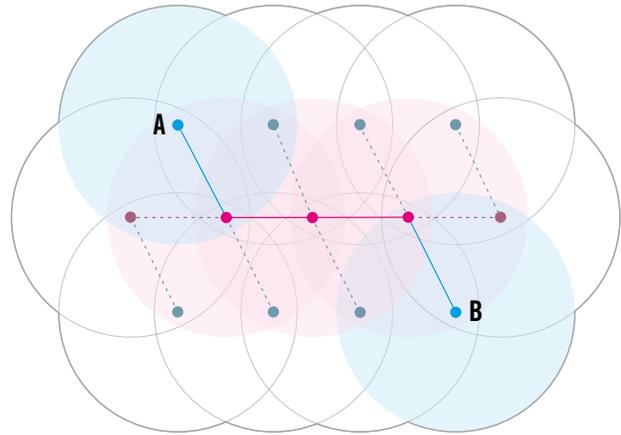
Ursprünglich sind die WLAN-Technologien, die heute unter Wi-Fi und WiMAX zusammengefasst werden, für den Ersatz oder die Ergänzung von Ethernet-Netzwerken vorgesehen gewesen. Anstatt aufwändiger Verkabelungen sollten Accesspoints die Verbindung zwischen den Computern und Servern herstellen. Um überhaupt den Betrieb eines Funknetzwerkes ohne regulatorische Hürden zu ermöglichen, beschränken sich die Wi-Fi-Netzwerke dabei auf lizenzfreie Frequenzbänder. Somit benötigt man nur die entsprechende Hardware und kann ein Funknetzwerk aufbauen. Diese Regulierungsfreiheit hat neben der steigenden Zahl mobiler Rechner zu einer enormen Verbreitung von WLANs geführt: von privaten WLANs mit einem Accesspoint über Hotspots, die öffentliche Räume abdecken, bis hin zu Netzwerken, die ganze Gebäudekomplexe abdecken. Gemein ist allen diesen Netzwerken, dass sie einen klassischen Aufbau besitzen. Im Falle eines Accesspoints der mehrere Endgeräte miteinander verbindet in einer sternförmigen Topologie oder mit mehreren Accesspoints die in einer Baumstruktur miteinander verknüpft sind oder gleichberechtigt auf einer Ebene als Backbone fungieren. Welche Struktur auch immer diese Netzwerke haben, sie ist hierarchisch und die Kommunikation läuft immer über zentrale Knoten. Selbst wenn Endgeräte im jeweiligen Empfangsbereich des anderen liegen, wird die Kommunikation immer über die Accesspoints laufen, was angesichts der knappen Übertragungskapazitäten eine Verschwendung ist.

Zudem kann so der Ausfall eines Netzknotens dazu führen, dass ganze Gebiete keinen Zugang mehr zum Netz haben. Ist das bei drahtgebundenen Netzwerken noch unvermeidbar beziehungsweise nur mit hohem infrastrukturellem Aufwand umgehbar, da es eben keine Sendezonen, sondern nur punktuelle Anschlüsse gibt, so bietet sich für die Funknetzwerke an, die Möglichkeit der Direktverbindungen zwischen jedem beteiligten Gerät zu nutzen. Die Formel dafür lautet Meshed Networking. Hierbei gibt es drei Ansätze.

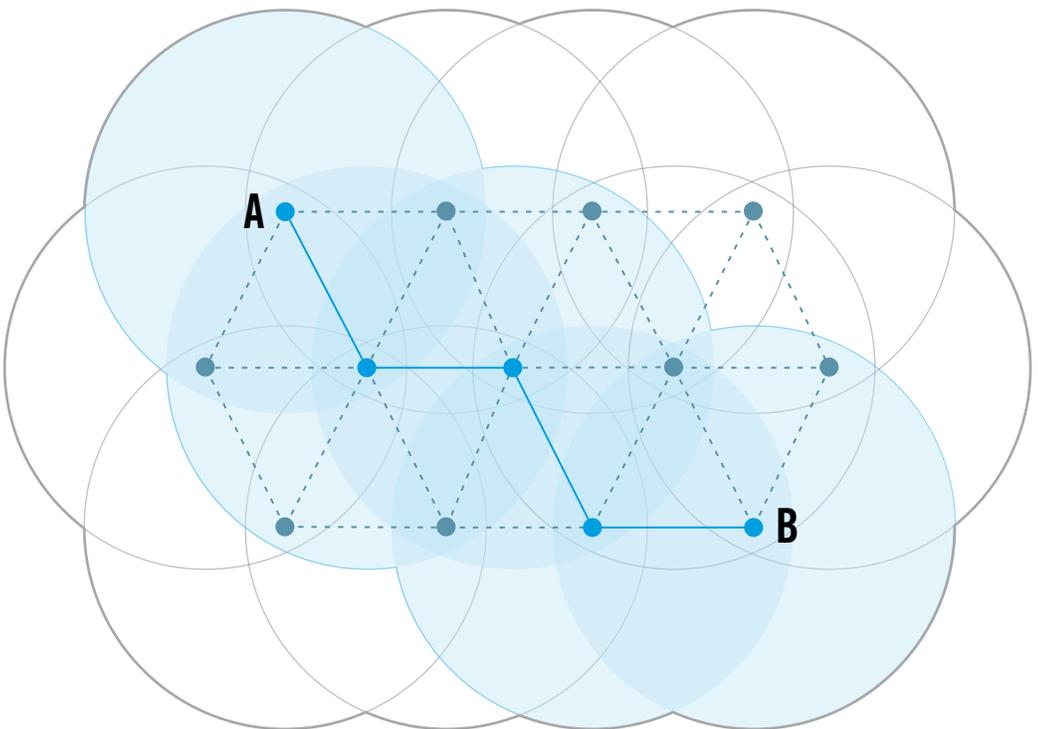
STAR NETWORK



INFRASTRUCTURE NETWORK



MESH NETWORK



MESHED INFRASTRUCTURE

Es werden feste Accesspoints installiert, die nicht mehr hierarchisch miteinander verbunden sind, sondern jeder Knoten kommuniziert mit jedem für ihn sichtbaren Knoten im ad-hoc Verfahren. Die Endgeräte verbinden sich jeweils mit einem Infrastrukturnoten. Roaming beim Übergang in den Sendebereich eines anderen Knotens ist möglich.

CLIENT PEER-TO-PEER

Jedes Gerät in einem Netzwerk ist gleichberechtigt und wird so nicht nur zum Sender und Empfänger, sondern auch zum Knoten. Eine Infrastruktur wird nicht benötigt. Das Netzwerk konfiguriert sich ständig im ad-hoc Verfahren neu, sobald ein Knoten hinzukommt, verschwindet oder seine Position ändert. Nachteil ist der erhebliche Protokoll-Overhead, der so entsteht, da jede Änderung permanent allen Beteiligten übermittelt werden muss.

MESHED INFRASTRUCTURE AND CLIENT

Dies ist im Prinzip die Kombination der Vorteile der beiden anderen Topologien. Eine zentrale Infrastruktur verbindet größere geographische Entfernungen und sichert die permanente Verfügbarkeit des Netzes. Zusätzlich können alle Geräte sich auch Peer-to-Peer verbinden und als Repeater aktiv sein.

2.4 REALISIERUNG EINES WMAN MIT WI-FI UND WIMAX

In den letzten zwei Jahren haben auf der ganzen Welt Projekte begonnen, WMANs zu realisieren. Je nachdem, welche Firma den Auftrag dazu erhalten hat, werden unterschiedliche Technologien verwendet. Neben den kommerziellen Ansätzen, wie etwa in Taipeh (Nortel/Wi-Fi), San Francisco (Earthlink, Google/Wi-Fi) oder Pakistan (Motorola/WiMAX), gibt es auch eine ganze Reihe privater Initiativen, wie in Berlin (www.freifunk.net) oder Seattle (www.seattlewireless.net).

Dies ist eine fast beliebige Auswahl aus einer rapide und unüberschaubar wachsenden Zahl von Projekten, die WMANs implementieren wollen. Dass dabei nicht nur WiMAX zum Einsatz kommt, das für solche großflächigen Netze konzipiert ist, liegt insbesondere auch daran, dass der Wunsch nach WMANs früher kam, als WiMAX verfügbar war. Auch wenn es mittlerweile

einige erste WiMAX-Netze nach 802.16d oder 802.16-2004 gibt, will beispielsweise Motorola für das riesige WMAN-Projekt in Pakistan auf Mobile WiMAX warten, das Ende dieses Jahres zertifiziert werden soll.

Auf der anderen Seite ist Wi-Fi-Technologie nicht nur seit Jahren auf dem Markt, sondern auch extrem günstig. Die privaten Stadtnetze etwa haben kein großes Budget, sondern setzen auf herkömmliche Consumer-Hardware, um ihre Netze zu errichten. Ebenso ist auch für aufwändigere Stadtnetze die Infrastruktur-Technik vergleichsweise billig und erprobt. Alle großen ICT-Firmen, ob Nortel, Motorola, Philips o.a., bieten komplette Systeme an, von der Verwaltungssoftware bis hin zum Endgerät. Um nicht einen Hersteller und seine Produkte bevorzugt darzustellen, wird nun im Folgenden ein mögliches WMAN und seine Implikationen anhand von Fragen und Antworten erläutert. Da sich die Angebote der verschiedenen Hersteller konzeptuell auch ähnlich sind, ist dies ein gangbarer Weg. Darüber hinaus gibt es auf den Webseiten der Hersteller eine ganze Reihe von Fallstudien. Die Links dazu finden sich im Anhang.

1. WARUM UND WOFÜR EINE FIXE INFRASTRUKTUR?

Diese Frage ist mit Ausblick auf die kommenden Wi-Fi Standards, die ad-hoc Mesh Networking implementiert haben werden, durchaus berechtigt. Die drahtgebundenen MANs und daran angeschlossene Wi-Fi APs könnten im Zusammenspiel mit den immer zahlreicher werdenden mobilen und fixen Wi-Fi-Clients ganz von selbst für eine vollständige Abdeckung einer Stadt reichen. Die privaten Initiativen, auch Mu-Fi genannt, bemühen sich, genau solche Netzwerke zu errichten, die ohne zentrale Steuerung und Betrieb auskommen, sondern einfach nur ein loser Verbund privat betriebener Accesspoints sind. Dieser Idee folgend, müssten einfach nur genug Teilnehmer sich anschließen, und das WMAN wäre vorhanden. Da dafür keine proprietären Technologien, sondern Standard Consumer-Hardware genutzt wird, ist sogar sichergestellt, dass jeder Zugriff darauf hat.

Ein großer Nachteil dieser ad-hoc Netzwerke ist aber das Fehlen jedweder Garantie auf Verbindung und Verbindungsqualität. Ohne einen zentralen Betreiber fällt zwar auch die Notwendigkeit weg, für den Netzzugang zu zahlen, dafür aber auch eine Anlaufstelle zur Sicherstellung der

Netzverfügbarkeit. Ebenso muss der Anschluss an das WAN/MAN finanziert werden. In heutigen Mu-Fis und Hot-Spots ist die Anbindung an das Internet über Endanschlüsse via DSL oder TV-Kabel gelöst. Die berühmte letzte Meile liegt immer noch in den Händen der TelCo-Provider, und aufgrund regulatorischer und finanzieller Probleme wird das auch so bleiben. Eine WiMAX-Infrastruktur wird sowohl eine Funküberbrückung für diese letzte Meile als auch alternative Routingmöglichkeiten anbieten. Und das sogar da, wo kein drahtgebundenes MAN liegt.

Ein weiterer Grund für eine fixe Infrastruktur ist die gewünschte Lokalisation, die Fixpunkte benötigt, um die Position eines Netzknotens genau bestimmen zu können. In einem rein mobilen ad-hoc Netzwerk ist zwar auch bis zu einer bestimmten Grenze die Ortung möglich, aber bei weitem nicht so exakt wie mit einer fixen Infrastruktur. So entsteht ein komplementärer Dienst zu GPS und Galileo, die prinzipbedingt in engen Straßenschluchten oder in überdachten Orten nicht funktionieren.

Hier wird noch einmal deutlich, dass lokale Wi-Fi-Netzwerke und großflächige WiMAX-Netzwerke als komplementäre Technologien zu verstehen sind. Aus diesem Aufbau ergeben sich einige Fragen, die im Folgenden gestellt und beantwortet werden.

2. WER BETREIBT DIE WMAN-INFRASTRUKTUR?

Diese Frage ist schon teilweise beantwortet, aber da sie wichtig ist, soll noch einmal darauf eingegangen werden. Eine WiMAX-Infrastruktur als Überbrückung der letzten Meile und stadtweites Angebot eines breitbandigen Mobilfunknetzes wird immer in den Händen eines TelCo-Providers sein. Da der TelCo-Markt immer weiter liberalisiert wird und regulatorische Eingriffe vermieden werden sollen, wird dieser Provider in den seltensten Fällen die öffentliche Hand sein. Aufgrund der Finanzierung solcher Projekte scheiden im Prinzip auch private Organisationen aus, da zwar die Hardware immer billiger wird, aber der Anschluss an das Internetbackbone immense Kosten nach sich zieht. Es bleiben letztlich nur gewinnorientierte Unternehmen als mögliche Betreiber übrig. Durch die vergleichsweise geringen Installationskosten eines solchen Netzwerks werden, wie heute schon bei den Mobiltelefonnetzen, mehrere Anbieter Netz anbieten. In Frage kommen hier im Prinzip alle Unternehmen, die heute schon in diesem Markt tätig sind.

3. WIE WERDEN SICH WMANS AUF ANDERE FUNKINFRASTRUKTUREN AUSWIRKEN?

WMANs sind nicht nur dazu geeignet, die letzte Meile per Funk zu überbrücken und das sprichwörtliche Evernet zur Verfügung zu stellen, sondern über sie wird es auch möglich sein, mittels VoIP zu telefonieren. Sie stehen damit in direkter Konkurrenz zu den Mobiltelefonnetzen, insbesondere den 3G-Netzen wie UMTS, deren besonderes Merkmal eigentlich die stark erhöhte Datenübertragungsrate sein sollte, die aber im Vergleich zu WiMAX wiederum gering ausfällt. Erst die gerade in der Entwicklung befindlichen 4G-Netze weisen WiMAX entsprechende Übertragungsraten auf.

Nach der Einschätzung von Analysten wird in den nächsten Jahren die gesamte Telekommunikation über IP-basierte Netzwerke ablaufen. Für die Netze heißt dies, dass eine Verschmelzung stattfinden wird und sie mehr in den Hintergrund rücken werden. Ob man nun telefonieren, auf das Internet zugreifen oder andere Dienste in Anspruch nehmen will, ob nun mobil oder über fix, es wird funktionieren. Welches Netz dann dabei genutzt wird, ist egal.

Insbesondere die Zahl und die Wichtigkeit der Festnetztelefone wird rapide abnehmen. Mobile Endgeräte nach dem UMA-Konzept werden sich in das gerade verfügbare Netz einwählen, was nach einer Übergangsphase immer ein IP-Netz sein wird.

4. WIE WERDEN SICH WMAN AUF PROVIDER- UND BEZAHLSTRUKTUREN AUSWIRKEN?

Geht man davon aus, dass die Netze, ob nun drahtgebunden oder Funk, in ihrer Funktionalität verschmelzen und gleichwertigen Zugriff auf die verschiedensten Dienste anbieten und das »Always-On« zur Selbstverständlichkeit wird, dann wird deutlich, dass heutig zeitbasierte Abrechnungsmodelle wenig Zukunft haben. Vor allem die Trennung zwischen Mobilfunkdiensten und Festanschlussdiensten wird im Zuge dieser Entwicklung verschwinden.

Weiterhin wird es zu einer Auflösung der Bindung von Diensten an einzelne Netze beziehungsweise Netzbetreiber kommen. Dazu werden vor allem VoIP-Dienste und andere Datendienste beitragen. Es ist anzunehmen, dass zukünftig eine Grundgebühr zu zahlen ist, um Zugang zum Netz zu bekommen. Oder, wie das Konzept von Earthlink und Google in San Francisco

vorsieht, dass ein langsamer Zugang kostenlos ist und für schnellen Zugang gezahlt werden muss. Das Always-On- Sein wird zu einer kostenlosen oder zumindest mit geringen Kosten verbundenen Selbstverständlichkeit.

Die Preise, vor allem für mobiles online- Sein, werden noch dramatisch fallen. Geld wird mit Bereitstellung der Infrastruktur nur noch in begrenztem Maße zu verdienen sein. Geld wird hauptsächlich mit Diensten und Serviceangeboten zu verdienen sein. Im Bereich Kommunikation machen etwa Skype oder SIP-Gate vor, wie solche Geschäftsmodelle aussehen können. Die Basisdienste sind kostenlos. Will man weitere Features wie einen Anrufbeantworter oder die Möglichkeit, herkömmliche Telefonanschlüsse zu erreichen, wird extra gezahlt.

Die Konkurrenz von solchen Diensten wird sicherlich einer der Gründe sein, warum die Betreiber der 2G und 3G-Mobilfunknetze sich nicht allzu sehr beeilen werden, flächendeckende IP-basierte Funknetze zu installieren. Denn in den aktuellen Bezahl- und Netzstrukturen sind diese fremden Angebote keine ernsthafte Alternative, und das momentane Geschäft kann noch eine Weile in Ruhe betrieben werden. Die steigende Zahl von Hot-Spots und Mu-Fis deutet aber an, dass es einen Bedarf gibt. Und wo es einen Bedarf gibt, werden sich Anbieter finden. Wenn es nicht die sind, die bereits am Markt sind, dann tun es andere. Dank der vergleichsweise geringen Kosten wird es auch kleineren Unternehmen möglich sein, solche Netze, wenn auch nur regional begrenzt, aufzubauen.²

5. WIRD ES SO BALD DAS EINE WIRKLICH ALLES VERBINDENDE NETZ GEBEN?

Ja und nein. Firmen und Institutionen werden auch zukünftig ein Interesse daran haben, ihre eigene geschlossene Infrastruktur zu haben, die nur über sorgsam überwachte Schnittstellen nach außen kommuniziert. Es wird zwar das große Evernet geben, aber parallel dazu auch geschlossene Netze, etwa für städtische Infrastruktur wie Informationstafeln, Überwachungskameras und ähnliches, die zwar auch auf WiMAX und Wi-Fi basieren können, aber oftmals weiterhin drahtgebunden sein werden, um die Angriffsmöglichkeiten zu minimieren. Viele Firmen haben etwa schon heute

² Als Beispiel für diese Entwicklung ist der Regionalprovider Urban Wimax in Großbritannien zu sehen. <<http://www.urbanwimax.co.uk/>> und <<http://www.techworld.com/mobility/news/index.cfm?NewsID=5599&inkc=0>>.

eindeutige Verbote, was die Nutzung von WLAN-Geräten angeht. Dies wird sich auch in Zukunft nicht ändern, aber die Notwendigkeit besteht auch einfach nicht.

6. WIRD DURCH DIE FUNKVERBINDUNGEN NICHT ALLES UNSICHERER?

Ja und nein. Ja, weil prinzipbedingt eine Funkverbindung viel leichter abgehört werden kann als eine drahtgebundene. Nein, weil unter der Voraussetzung, dass alle Geräte sowieso über das Internet verbunden sind, die Angriffsfläche gleich bleibt. Unter Berücksichtigung der Tatsache, dass heute der größte Teil der Internetkommunikation unverschlüsselt abläuft und in Wi-Fi und WiMAX-Netzen eine Verschlüsselung Standard sein wird, wird die Kommunikation in gewisser Hinsicht sogar sicherer werden. Dass das Internet im Allgemeinen unter Sicherheitsproblemen leidet, wird auch durch Wi-Fi und WiMAX nicht vermieden. Die Integrität des Internets ist ein permanentes Problem, das sich hinsichtlich der immer stärkeren Nutzung in der Summe aber sicherlich verstärken wird.

7. FÜHRT DIESES EVERNET NICHT ZUR TOTALEN ÜBERWACHUNG?

Nicht mehr als heute – eher weniger. Während heute jedes Mobiltelefon, sobald es eingeschaltet ist, sich ins Netz einwählt und darüber lokalisierbar ist, wird in den vermaschten WMANs die Netzverbindung auch oft über private Knoten realisiert werden und nicht unmittelbar über eine lokalisierbare Infrastruktur. Eine zentrale Anlaufstelle zur Abfrage von Lokalisationsdaten wird es also oft nicht mehr geben. Zwar wird jedes Gerät immer noch eindeutig identifizierbar sein, aber etwa die IP-Adresse wird sich ständig ändern, wenn man sich durch ein vermaschtes Netz bewegt. Zusätzlich werden Daten wie die MAC-Nummer, die jedes Gerät eindeutig identifiziert, nicht über das gesamte Netzwerk gesendet. Durch die notwendige Verschlüsselung der Funkverbindungen, wird es aber jenseits der IP-Adresse mehr Identifikationsmöglichkeiten geben, wenn nicht auf Session Based Keys gesetzt wird. Man wird also always-on sein, aber oft unsichtbar, zumindest was die Position im Detail angeht.

Hinsichtlich dieser absehbaren Entwicklung sind zwar gesetzliche Regelungen denkbar, die Behörden auch den Zugriff auf private Geräte direkt ermöglichen, allerdings wäre eine solche Lösung ein so radikaler Einschnitt

in die Persönlichkeitsrechte und die informationelle Selbstbestimmung, dass ein solcher Schritt hoffentlich nie erfolgt. Andererseits ist es möglich, wenn es gewollt ist, sehr exakt die Position zu bestimmen, was für viele Dienste Grundvoraussetzung ist. Auch hier stellt sich vor allem die Frage, wem solche Daten wie zur Verfügung stehen.

8. WERDEN PRIVATE MESHED NETWORKS ZU EINEM ZWEITEN INTERNET FÜHREN?

Möglich. Schon heute ist es mit Tunnelingprotokollen möglich, virtuelle Netzwerke über das Internet zu errichten. Je nachdem, wie sich die gesetzliche Lage in Zukunft entwickelt, bieten die privaten Mesh-Netze tatsächlich eine interessante Alternative, um der Überwachung des Datenverkehrs auf einfache Art und Weise zu entgehen. Allerdings steht es zu erwarten, dass mit kommenden Funknetztechnologien, die auf ad-hoc Meshing basieren und damit die fest installierte Infrastruktur immer unwichtiger werden lassen, auch entsprechende Kontrollmöglichkeiten implementiert werden. In den nächsten Jahren ist allerdings weder absehbar, dass sich die privaten Netze wirklich flächendeckend ausbreiten, noch dass sie sich in ihrer Benutzbarkeit und Implementation so sehr vereinfachen, dass auch ein Technikleie sie nutzen kann.

9. SIND WIMAX UND WI-FI NICHT ZU LANGSAM, UM DAS EVERNET ZU REALISIEREN?

Im Prinzip ja. Gerade WiMAX bietet mit den momentan realisierbaren 40MBit definitiv zu wenig, um drahtgebundene Breitbandanschlüsse in dicht besiedelten Regionen zu ersetzen. Forschung und Entwicklung gehen aber kontinuierlich weiter, und es wird für die nächsten fünf Jahre erwartet, dass die Übertragungsraten für Wi-Fi-Netze auf bis zu 500MBit gesteigert werden können, bei gleichzeitiger Abwärtskompatibilität zu heutigen Standards und entsprechenden Geräten.

Zudem sind Wi-Fi und WiMAX schon heute den anderen Mobilfunknetzen, was die Datenübertragungsrate angeht, weit überlegen. Für die meisten mobilen Anwendungen ist also schon mit den heutigen Standards mehr als genug Übertragungsrate vorhanden im WMAN/WLAN. Ebenso wird sich die Netzlast in Meshed Networks besser verteilen, sodass die Chance, einen einzelnen Knoten zu überlasten, geringer wird.

10. WAS HAT DAS ALLES MIT UBIQUITOUS COMPUTING ZU TUN?

Das »Always-On« und die damit verbundene Vereinheitlichung der Kommunikation betrifft nicht nur die Kommunikation zwischen Menschen. Dieselbe Infrastruktur wird auch die Kommunikation zwischen Objekten und Diensten ermöglichen. Die Schnittstelle dazu werden WPAN AP sein, die als zentrale Schnittstelle zwischen WMAN/WLAN und WPAN/NFC fungieren werden. Vergleichbar mit Mobiltelefonen heute, die auch im Nahbereich mittels Bluetooth oder IrDA kommunizieren können und als solche als Vorläufer dieser Netzstrukturen gelten können.

Die Grundvoraussetzung für eine Menge Anwendungen wird die Möglichkeit sein, über solche Schnittstellen auf entfernt gespeicherte Daten zuzugreifen. WiMAX/Wi-Fi-Netze bieten die dafür notwendige Infrastruktur.

11. WANN WERDEN WMANS DENN ENDLICH INSTALLIERT?

Momentan gibt es weltweit eine ganze Reihe von Projekten zur Realisierung von WMANs. Diese ersten Pilotprojekte werden sicherlich aufmerksam beobachtet. Speziell in Deutschland dürfte es noch einige Zeit dauern, bis WiMAX-WMANs installiert werden. Zu hoch waren die Investitionen der TelCo-Unternehmen für die GSM- und UMTS-Netze, als dass sie diese Netze nun einfach abbauen und WiMAX überall installieren. Dank des deregulierten Marktes ist es aber wahrscheinlich, dass andere Anbieter beginnen werden, komplementäre Netze zu errichten. Der Wettbewerb unter den Betreibern wird sich so verstärken. Dabei müssen Wi-Fi und WiMAX-Netze erst noch beweisen, dass sie die bessere Alternative sind. Ein Schlüsselrolle wird dabei den Endgeräten zukommen, die die Nutzung dieser Netze ermöglichen. Mobiltelefonieren ist heute vergleichsweise einfach zu bewerkstelligen. Diese Einfachheit muss erhalten oder noch verbessert werden. Neben dieser Kernkompetenz der Mobilfunknetze wird die Implementierung neuer Dienste ein weiteres Kriterium für den Erfolg neuer Netze sein. Viele dieser Applikationen lassen sich auch mit UMTS-Netzen abbilden, was ebenso ein Hinderungsgrund für die großflächige Installation solcher Dienste sein kann.

Als drahtlose Alternative für Breitbandanschlüsse wird WiMAX in regional begrenzten Räumen sicherlich schneller implementiert. In einem Jahr wird in diesem Anwendungsfall sicherlich mehr Klarheit bestehen.

2.5 HOCHMOBILE WLANS

Neben der Entwicklung zu einem immer verfügbaren WMAN, auf Basis von Wi-Fi und WiMAX, ist der Bereich der hochmobilen Netzwerke eine besondere Herausforderung. Bewegt sich ein Netzteilnehmer, wird es besonders schwierig, die Verbindung aufrechtzuerhalten – ein physikalisches Problem, das alle Funknetze betrifft. Ist die Bewegung eines Fußgängers noch vernachlässigbar, wird es für Autos oder gar Hochgeschwindigkeitszüge wie den ICE schon sehr viel schwieriger, eine permanente Verbindung aufrechtzuerhalten.

Momentan arbeitet in Europa ein Konsortium, in dem viele europäische Autohersteller vertreten sind, an einer gemeinsamen Lösung für ein Car2Car-Netz. Wie der Name bereits andeutet, wird auch hier versucht, ein infrastrukturloses Netz zu realisieren. Hinsichtlich des Verkehrs in der Stadt ist dies besonders interessant, da auf diese Art die ausschließlich für Verkehrsteilnehmer relevanten Informationen über ein eigenes Netz kommuniziert werden können, ohne dass das eigentliche Stadtnetz damit belastet wird. Die Interoperabilität wird aber gewährleistet bleiben, da auch das Car2Car-Konsortium eine 802.11-Standardisierung anstrebt. Denkt man diesen Ansatz noch einen Schritt weiter und dehnt ihn auf die Verkehrsinfrastruktur wie Ampel, Parkhäuser und Verkehrsleitzentrale aus, werden viele Anwendungsmöglichkeiten deutlich. Echtzeit-Staumeldungen oder mobile Mautzahlungen ohne zusätzliche Systeme sind nur einige davon.

3 WIRELESS PERSONAL AREA NETWORK & NEAR FIELD COMMUNICATION

Das Wireless Personal Area Network (WPAN) und die Near Field Communication (NFC) sind eng miteinander verwandt. Unter WPAN werden hauptsächlich Funknetzwerkprotokolle wie Bluetooth, ZigBee oder ähnliche zusammengefasst. Dabei ist das »Personal« leicht missverständlich. Hiermit ist nicht zwangsläufig ein personenbezogenes Netzwerk gemeint, sondern vielmehr die Reichweite dieser Funktechnologien, die nur wenige Meter beträgt. Unter NFC werden die Technologien zusammengefasst, die eine Integration von RFID in die bereits existierenden ICT-Strukturen ermöglichen. Es ist damit nicht die RFID-Smartcard gemeint, sondern die Integration eines RFID-Transponders in etwa ein Mobiltelefon. Insofern ist NFC nur ein anderes Wort für RFID-Kommunikation, möglicherweise geprägt, um dem mittlerweile negativ belegten Begriff »RFID« aus dem Weg zu gehen. Der wesentliche Unterschied ist, dass die WPAN-Technologien vorsehen, dass jeder beteiligte Netzknoten von sich aus senden beziehungsweise die Kommunikation initiieren kann, während das bei NFC prinzipbedingt nur der Transponder kann, auf den dann die RFID-Chips reagieren. NFC kann als Erweiterung des WPANs für entsprechende Anwendungsfälle gesehen werden. Da RFID im entsprechenden Kapitel schon ausführlich besprochen wurde, wird hier nicht weiter darauf eingegangen, taucht in den Anwendungsbeispielen aber wieder auf, um die Zusammenhänge mit den WPAN-Technologien deutlich zu machen.

Einer der wesentlichen Gründe für WPAN-Systeme war und ist die steigende Zahl von Geräten, die miteinander kommunizieren sollen. Anstatt ein Kabel als Verbindung zu nutzen, was vor allem bei mobilen Geräten lästig oder je nach Einsatzform gar nicht möglich ist, wird die Verbindung per Funk hergestellt. Die heute gebräuchlichste Funktechnologie ist aktuell Bluetooth. Bluetooth ist standardisiert als IEEE 802.15.1 und ist seit etwa drei Jahren als Kommunikationsprotokoll in breiter Anwendung. Bluetooth definiert drei Geräteklassen, die sich durch die Sendeleistung und damit Reichweite auszeichnen. Klasse 1 Geräte können bis zu 100m weit funken, während Klasse 2 auf etwa 10m und Klasse 3 auf 1m beschränkt ist. Klasse 1 Geräte sind so gut wie nicht anzutreffen, da sie für die Anwendungen im WPAN nicht notwendig sind.

Am verbreitetsten sind Klasse 2 Geräte, die hinsichtlich Reichweite und Stromverbrauch den besten Kompromiss bieten. Der aktuelle Standard 1.2 sieht Übertragungsgeschwindigkeiten bis zu 723kbit vor. Dies klingt im Vergleich zu anderen Funktechnologien wenig, ist aber für viele Anwendungen völlig ausreichend. Heute wird die Bluetooth-Schnittstelle vor allem für die Kommunikation zwischen Mobiltelefon und Computern genutzt, um Daten abzugleichen, oder als Verbindung der Peripheriegeräte wie Headsets, Fernbedienungen und andere Eingabegeräte. Bluetooth ermöglicht dabei eine ad-hoc Vernetzung der Geräte. Dem dabei auftretenden Problem, dass auch Verbindungen zwischen Geräten hergestellt werden könnten, die gar nicht gewünscht sind, kann durch die Festlegung eines Schlüssels, der den autorisierten Geräten gegeben wird, vorgebeugt werden.

Dass Bluetooth-Netze mit ihrer ad-hoc Vernetzung, auch im öffentlichen Raum, kritisch sein können, wurde bereits mit einem Proof-Of-Concept-Virus gezeigt, der Mobiltelefone infizieren kann und sich über die Bluetooth-Schnittstelle verbreitet. Ebenso zeigt sich auch das Problem der Authentifizierung von gewollten Verbindungen durch das Konzept des »Bluejacking«, indem ein fremdes Gerät vorgibt, ein bekanntes zu sein, und eine bereits aufgebaute Verbindung auf sich umleitet.

Viele der Probleme, die bei anderen Technologien und Funknetzen bislang eher theoretischer Natur sind, sind bei Bluetooth akut. Als erstes mobiles infrastrukturloses ad-hoc-Netz wird die Implementation von zuverlässiger und sicherer Authentifikation und Verschlüsselung, die auch noch praktikabel anwendbar ist, zur Nagelprobe für weitere ad-hoc Netzwerke, zu denen bald auch WMANs zu Teilen gehören können.

Während Bluetooth aufgrund geringer Herstellungskosten, kleinen Formfaktors, geringen Stromverbrauchs und nicht zuletzt wegen der ad-hoc-Vernetzung sich besonders für mobile Anwendungen eignet, kann es als Verbindung zwischen Geräten nicht alle Anwendungsfälle in einem WPAN abdecken. Dort, wo größere Datenmengen zu übertragen sind, bleibt es bislang außen vor und dort, wo extrem geringer Stromverbrauch gefragt und nur sehr geringe Datenmengen anfallen, ist Bluetooth überproportioniert. Für diese beiden Anwendungsprofile wird an komplementären Technologien gearbeitet.

Für Verbindungen zwischen Geräten, die große Datenmengen übertragen, wird an UWB oder Wireless USB³ (WUSB 802.15.3a) gearbeitet. Dabei soll dieser Funkstandard, wie Wireless-USB bereits sagt, überall da zum Einsatz kommen, wo heute drahtgebundene USB-Verbindungen zum Einsatz kommen, etwa zwischen Computer und Drucker oder externer Festplatte. Die Übertragungsraten sollen dabei im Nahbereich von etwa 3m denen vom herkömmlichen USB entsprechen, also 480Mbit betragen. Das UWB-Konsortium denkt jedoch daran, mit solchen Funkverbindungen nicht nur USB, sondern alle Verbindungsarten im Elektronik- und IT-Bereich zu ersetzen, also etwa auch die Verbindung zwischen Computer und Monitor oder zwischen Mediaplayer und Fernseher. Geräte mit einer WUSB-Schnittstelle werden in naher Zukunft auf den Markt kommen und werden so die Integration von Computer- und Unterhaltungselektronik weiter vorantreiben. Aus dem »Auspacken, anschließen, einschalten, einrichten, funktioniert« soll ein »Auspacken, einschalten, funktioniert« werden, da die Geräte die Kommunikation im ad-hoc Verfahren selber aushandeln.

Während sowohl Bluetooth als auch WUSB ganz klar als ICT im herkömmlichen Sinne zu sehen sind, zielt ZigBee viel stärker auf Integration als Kommunikationsnetz für Ambient Intelligence oder Ubiquitous Computing. ZigBee soll sehr billig und einfach zu integrieren sein und dabei fähig, selbstständig im ad-hoc Verfahren Meshed Networks aufbauen zu können. ZigBee ist zwar darauf ausgelegt, möglichst wenig Strom zu verbrauchen, bleibt aber dennoch davon abhängig, wird also primär in Systemen und Geräten zum Einsatz kommen, die ohnehin eine Stromversorgung benötigen. Speziell im Bereich der Hausautomation ist ZigBee nur eine von vielen Varianten für die Kommunikationsstruktur. Vorteil von ZigBee ist vor allem, dass es wie die anderen IEEE Standards offengelegt ist und somit nicht proprietär an die Hardwaresysteme eines Herstellers gebunden ist. Die so wichtige Interoperabilität, die Grundvoraussetzung für UC im Allgemeinen und Meshed Networks im Speziellen ist, kann nur durch solch offene Standards erreicht werden.

3 Wichtig ist hier die Unterscheidung zwischen Wireless USB und WirelessUSB™. Zweiteres ist eine proprietäre Technologie mit maximalen Übertragungsraten von 1Mbit und am ehesten mit Bluetooth zu vergleichen.

Zusammenfassend kann gesagt werden, dass es im Bereich der räumlich begrenzten Netzwerke oder eben WPAN für jeden erdenklichen Kommunikationsfall mittlerweile offene Funkstandards gibt. Dank der Konzeption der verschiedenen Netzwerke ist dabei ein Ineinandergreifen problemlos möglich. Allerdings wird an den bereits existierenden Lösungen im Bluetooth-Bereich deutlich, dass der Schutz dieser Netzwerke alles andere als trivial ist. Gerade die Fähigkeiten, selbstständig Netzwerke aufzubauen, die Bluetooth so komfortabel und dadurch beliebt macht, ist gleichzeitig das größte Problem. Dieses Problem wird noch größer werden, wenn die Kommunikation auf diese Art und Weise zur Regel wird und nicht wie heute noch der Ausnahmefall ist. Obwohl beispielsweise viele Mobiltelefone eine Bluetooth-Schnittstelle besitzen, ist die Nutzung äußerst gering.⁴ Noch ist es also ein gangbarer Weg, die potentielle Gefährdung durch Ausschalten von Bluetooth zu eliminieren und es nur im bewussten Anwendungsfall zu aktivieren. Dadurch werden aber eben auch die Vorteile von ad-hoc-Netzen wieder nihilisiert und letztendlich auch die Idee vom allgegenwärtigen automatisierten Informationsaustausch.

Der zurückhaltende Gebrauch der bereits existierenden WPAN-Technologien zeigt aber auch, dass in vielen Bereichen der Wunsch oder Bedarf an zusätzlichen Kommunikationsmöglichkeiten möglicherweise gar nicht so groß ist beziehungsweise das Vertrauen in die Technologien nicht vorhanden ist. Am Beispiel des Mobiltelefons und der Kontaktspeicherung zeigt sich dies deutlich. Die mündliche Übermittlung der Telefonnummer authentifiziert sie gleichzeitig auch. Nach einem ersten Rückruf haben dann beide beteiligten Personen gegenseitig die Telefonnummer gespeichert, identifizierbar gemacht, verifiziert und autorisiert. Ein sehr komplexer Vorgang also, der als Automatismus mit WPAN-Technologien nur schwer nachzuvollziehen ist.

4 Diese Einschätzung entstammt einer nicht repräsentativen Umfrage zur Nutzung von Bluetooth beziehungsweise dessen Verfügbarkeit. Von den 30 befragten Mobiltelefonbesitzern hatten zwar 18 ein bluetoothfähiges Mobiltelefon, aber nur 4 nutzten Bluetooth auch aktiv, allerdings ausschließlich zum Abgleich zwischen Computer und Mobiltelefon. Als Kommunikationsschnittstelle zwischen Mobiltelefonen nutzte es niemand.

4 RFID

Kaum einer Technologie wird momentan so viel Potential zugesprochen, unser Alltagsleben zu verändern, wie RFID. Dabei ist RFID in technischer Hinsicht unspektakulär, eröffnet aber eben im Zusammenspiel mit anderen ICT viele Anwendungsmöglichkeiten. Radio Frequency Identification ist, wie der Name schon sagt, für die Identifikation per Funk gedacht und sollte als AIDC-Technologie (Automatic Identification and Data Capture) bestehende Identifikationssysteme ablösen. Der große Vorteil gegenüber bestehenden AIDC-Systemen wie Barcodes oder Magnetstreifenkarten ist die Funkübertragung. Es ist weder eine Sichtverbindung notwendig, noch muss ein RFID-Tag durch ein Lesegerät gezogen werden, um ausgelesen werden zu können. Zudem ist die Fehlerquote beim Auslesevorgang sehr gering, da weder Verschmutzung noch Abnutzung auftreten.

4.1 AKTIV/PASSIV

Generell werden zwei Typen von RFID-Technologien unterschieden. Die aktiven RFID-Tags besitzen eine eigene Stromversorgung, und die passiven nutzen die Sendeenergie des Transponders, um aktiv zu werden. Generell ist ein RFID-System so aufgebaut, dass es einen Transponder gibt, der die Kommunikation initiiert, und einem RFID-Chip, der an dem zu identifizierenden Objekt angebracht ist. Ohne den Transponder bleiben diese RFID-Chips, ob nun passiv oder aktiv, stumm, erst wenn sie eine Anfrage bekommen, reagieren sie. Der Transponder startet nicht nur die Kommunikation, sondern stellt auch die Schnittstelle zu den Informationsverarbeitungssystemen dar. Neben fest installierten Systemen als Passierstellen gibt es auch mobile Lösungen, der Oberbegriff hier ist dann Near Field Communication (NFC).

4.2 FREQUENZBEREICHE UND IHRE NUTZUNG

Neben der Unterscheidung »passiv und aktiv« ist eine wesentliche Unterscheidung der Chips die genutzte Frequenz. Dabei kristallisieren sich drei Bänder als meistgenutzte heraus. LF-Systeme nutzen das Band von 125-135 kHz, HF-Systeme nutzen das 13,56 MHz-Band, und schließlich nutzen UHF-Systeme verschiedene Bänder zwischen 868 und 915 MHz. Für die meisten aktuellen Anwendungen, besonders in Logistik-Systemen, wird aber das 13.56 MHz-Band genutzt.

Die am häufigsten eingesetzten HF-RFID-Chips können heute bis zu 1024Bit speichern, was 128Byte entspricht. Dabei ist nicht unbedingt der Speicherplatz auf dem Chip der limitierende Faktor, sondern die Übertragungsrate und -dauer, die sich aus der Sendefrequenz und der Sendeenergie ergeben. Prinzipbedingt können deshalb auf einem RFID-Chip immer nur sehr begrenzt Daten gespeichert werden. Dies ist einer der Hauptgründe, warum an RFID-Systemen mit höheren Sendefrequenzen gearbeitet wird.

Die Unterscheidung zwischen den Bändern ist wichtig, da für verschiedene Anwendungsfälle die unterschiedlichen Vor- und Nachteile der Bänder wichtige Kriterien sind. Beispielsweise sind die UHF-Systeme nicht für die Tier-ID-Systeme geeignet, da die UHF-Frequenzen äußerst effektiv von Wasser absorbiert werden, woraus nun einmal alle Lebewesen hauptsächlich bestehen. Andererseits benötigt das Senden auf niedrigen Frequenzen mehr Energie, was in einer geringeren Lesereichweite resultiert beziehungsweise größere Antennen erforderlich macht. Aus diesem Grund wird momentan auch an RFID-Chips gearbeitet, die auf dem 2,45 GHz-Band funken. Mit solchen Chips wäre es etwa möglich, Geldscheine mit einem RFID-Chip zu versehen.⁵ Als Antenne würde dann der Sicherungsmetallstreifen genügen. Ebenso reduziert sich mit der Frequenz auch die Datenrate, was ebenso ein Ausschlusskriterium sein kann. Tatsächlich gibt es eine Menge technischer Schwierigkeiten beim Einsatz von RFID-Systemen, die jetzt nicht im Detail erläutert zu werden brauchen.

5 Siehe <<http://www.heise.de/newsticker/meldung/69246>>

4.3 VORTEILE DER AKTIVEN RFID-CHIPS

Die aktiven RFID-Chips sind nur für wenige Anwendungen interessant. Die große Diskussion geht um die passiven Chips. Diese werden nun genauer erläutert. Dadurch, dass die passiven Chips keine eigene Stromversorgung benötigen, haben sie den großen Vorteil einer extrem hohen Lebensdauer, die im Prinzip nur durch die Korrosion des Chips beschränkt ist. Ebenso können sie sehr klein werden. Die einzige Begrenzung ist die Größe der Empfangs- und Sendeantennen. Sie können für HF- und UHF-Chips vor allem sehr flach werden, was sie für die Nutzung in Karten oder Labels prädestiniert. Die Herstellungskosten für einen solchen RFID-Chip betragen momentan etwa 8–10 Eurocent. Dieser Preis wird noch weiter fallen, je nach Chipart bis auf Zehntel Eurocent.

Was die RFID-Technologie so attraktiv macht, ist nicht allein die Möglichkeit der kontaktlosen und extrem fehlerfreien Identifikation, sondern auch die Möglichkeit, Informationen nicht nur auslesen zu können, sondern auch Informationen auf den Chip zu schreiben. Diese Fähigkeit eröffnet der RFID-Technologie eine Fülle an Anwendungen, die weit über die bloße Identifikation hinausgehen. RFID-Technologie kann so in vielen Bereichen Anwendung finden und wird tatsächlich auch bereits heute an vielen Stellen benutzt. Bevor nun exemplarisch einige Anwendungen vorgestellt werden, gibt es einen Überblick über die Vorteile von RFID:

1. Sehr klein.
2. Kontaktloses Auslesen.
3. Geringe Fehlerquote beim Auslesen.
4. Kostengünstig zu produzieren.
5. Kann Daten nicht nur einmal speichern und wiedergeben, sondern auch verarbeiten und wieder schreiben.
6. Benötigt keine eigene Stromversorgung.
7. Die Systeme können besser vor Umweltbedingungen geschützt werden, da kein Kontakt notwendig ist.

4.4 ANWENDUNGEN

TIERIDENTIFIKATION

Tieren wird ein LF-Chip implantiert, der sie eindeutig identifizierbar macht. Dies ist für Haustiere in EU-Ländern, wenn sie über eine Grenze mitgenommen werden sollen, Pflicht, ermöglicht aber auch bei Nutztieren die lückenlose Identifikation der Herkunft und des Transports. Zudem sind RFID-Chips fälschungssicherer als herkömmliche Verfahren zur Tieridentifikation wie Brandzeichen oder Ohrringe.

TRANSPORTSYSTEME

RFID-Systeme ermöglichen in der Logistik beschleunigte und fehlerfreie Abläufe. Das fehleranfällige und relativ zeitintensive Auslesen von Barcodes entfällt. Waren durchlaufen mehrere RFID-Passagen, die, ohne den Warenstrom aufhalten zu müssen, die momentane Position der Lieferung auf Richtigkeit überprüfen können. Werden nicht nur Container oder Paletten mit RFID-Chips ausgestattet, sondern auch einzelne Produkte, kann die Vollständigkeit der Ware überprüft werden, ohne alles öffnen zu müssen.

ZUGANGSKONTROLLE

Im Gegensatz zu Kontaktchipkarten können RFID-Smartcards auch aus einiger Entfernung ausgelesen werden und so die Zugangsberechtigung feststellen. Vorteil ist der schnellere Lesevorgang und die Abnutzungsfreiheit. Mit implantierten RFID-Chips fällt in einem solchen Szenario die Notwendigkeit einer Extrakarte weg. Sie kann weder verloren noch gestohlen werden.

ARCHIVIERUNG/LAGERUNG

Bei der Archivierung und Indexierung von etwa Büchern sind RFID-Systeme Barcode- oder Magnetstreifensystemen überlegen, da sie weder Kontakt noch Sichtverbindung benötigen. Die Position des gesamten Lager- oder Archivinhalts kann mit systematisch platzierten Transpondern permanent in Echtzeit überwacht werden. Falsche Einsortierung ist nicht mehr möglich.

WARENWIRTSCHAFTSSYSTEME

Neben den Logistiksystemen bietet RFID auch für Warenwirtschaftssysteme interessante Anwendungen. Etwa das Warenregal, das seinen Füllstand mitteilt, diesen mit dem Lagerwarenbestand abgleicht und automatisch neue Waren ordert. Der in Deutschland bekannteste Versuch dürfte der Future Store in Rheinberg sein.⁶

SMARTCARDS FÜR BEZAHLSYSTEME

Die Bezahlvorgänge mit kontaktlosen Smartcards können enorm beschleunigt werden gegenüber den fehleranfälligen Magnetstreifenkarten.

SENSORSYSTEME

Die Miniaturisierung der Halbleiter betrifft nicht nur informationsverarbeitende Systeme. Auch Sensoren verschiedenster Art können heute sehr klein werden. Fügt man RFID und Sensoren zusammen, hat man sehr kleine Messsysteme, die auch an Stellen platziert werden können, die heute nur schwierig zu erreichen sind beziehungsweise bei denen die Kommunikationsverbindung mit den Informationsverarbeitungssystemen nicht leicht herzustellen ist. Ein Beispiel wäre die Anbringung solcher Minisysteme in Autoreifen, die permanent den Reifendruck prüfen. Vielfach gibt es schon solche Systeme, die Vorteile der externen Stromversorgung und der preisgünstigen Herstellung sind jedoch erst mit RFID zu implementieren.

DER INTELLIGENTE MEDIZINSCHRANK

RFID-Etiketten an Medikamenten können nicht nur deren Identifikation sicherstellen, sondern auch die Beachtung etwa der Einnahmeverordnung und des Verfallsdatums. Zudem könnte ein intelligenter Medizinschrank vor versehentlicher oder unbewusster Einnahme von unverträglichen Medikamentenkombinationen warnen. Im Gegensatz zu den anderen hier vorgestellten Anwendungen ist der intelligente Medizinschrank jedoch nur eine Idee, wie der intelligente Kühlschrank. Aber das Beispiel zeigt auf, in wie vielen Bereichen RFID einsetzbar ist.

6 siehe <<http://www.future-store.org>>

EPASS

In vielen Ländern, auch in Deutschland, wird an maschinenlesbaren Reisepässen gearbeitet beziehungsweise sie werden bereits eingeführt. Der große Vorteil gegenüber Magnetstreifen und Kontaktchips soll hier die bessere Haltbarkeit sein, da der ePass 10 Jahre gültig ist und die Kontaktchips eventuell nicht so lange funktionieren. Speziell bei solchen sehr datenschutzempfindlichen Anwendungen zeigen sich aber deutliche Probleme der RFID-Technologie, wenn es um die Kontrolle des Lesevorgangs geht. So wird die Übertragung nicht nur verschlüsselt, sondern der Schlüssel ist nur über eine visuell auslesbare Machine Readable Zone (MRZ) zu erlangen, wie sie schon heute in Reisepässen vorhanden ist. Dies soll verhindern, dass der RFID-Chip unbemerkt ausgelesen wird. Dass ein solcher Technologiebruch notwendig ist, um wirklich effektiv zu verhindern, dass der RFID-Chip unbemerkt ausgelesen werden kann, zeigt, dass die heute existierenden RFID-Technologien äußerst unsicher sind. Zudem wurde in Versuchen gezeigt, dass der eigentlich stark reglementierte Übertragungsvorgang, der ePass wird in das Lesegerät gelegt und aus einer Entfernung von nur 10cm ausgelesen, dennoch aus mehreren Metern Entfernung abgehört werden kann. Die verwendeten DES-Verschlüsselungsalgorithmen geben eine effektive Schlüssellänge von 56Bit. Es wurde aufgezeigt, dass dieser Schutz sich in wenigen Stunden knacken lässt. Insgesamt stellt sich die Frage, bei solch kritischen Anwendungen, ob Funktechnologien überhaupt angewendet werden sollten oder wie stark eine Verschlüsselung mindestens sein muss, um ein großes Maß an Sicherheit zu gewährleisten, zumal die Vorteile der Funkübertragung beim ePass ad absurdum geführt werden, da nach wie vor visueller Kontakt hergestellt werden muss.⁷

⁷ Informationen zum ePass siehe <<http://www.epass.de>> und <http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/ePass_Biometrie/Hintergrundinfo_ePass.html> und hier die Nachricht zum Abhören und entschlüsseln des Lesevorgangs <<http://www.heise.de/newsticker/meldung/69127>>

4.5 DIE NACHTEILE VON RFID

Doch wie jede andere Technologie hat auch RFID nicht nur Vorteile, sondern auch systemimmanente Schwächen. Besonderes Augenmerk legen die Kritiker von RFID dabei auf den größten Vorteil von RFID, nämlich die Funkkommunikation. Denn RFID-Chips können praktisch jederzeit ausgelesen werden, auch in Situationen, in denen das nicht gewünscht ist. Mit einem RFID-Transponder ausgestattet, kann im Prinzip jeder jederzeit unbemerkt einen RFID-Chip auslesen. Kombiniert man das mit der Möglichkeit der aufgrund der Bauform und Kontaktlosigkeit möglichen versteckten Anbringung von RFID-Chips, baut sich so ein Szenario der permanenten unsichtbaren und unkontrollierbaren Überwachung und Profilerstellung auf.

In den meisten Anwendungsfällen von RFID ist momentan eine Kontrolle der Leseberechtigung nicht implementiert, wenn sie auch als Konzept existiert.⁸ Die bereits enthaltene Funktion, einen RFID-Chip zu deaktivieren, etwa wenn eine Ware gekauft wurde und der Kunde das Geschäft verlässt, wird allgemein als unzureichender Schutz vor Datenspionage gesehen, was nachvollziehbar ist, da sich alles, was sich ausschalten lässt, auch wieder einschalten lässt. Da das Ausschalten über die RFID-Kommunikation geregelt ist und kein weiteres System dafür notwendig ist, lässt sich also ein RFID-Chip auch so wieder einschalten. Der gangbare Weg über einen Medienbruch wie die Verschlüsselung im ePass, deren Schlüssel nicht über RFID kommuniziert wird, hat Grenzen, wie schon erläutert wurde. Zwar verhindert diese Verschlüsselung, dass ein ungewollter Lesevorgang stattfindet, aber ein autorisierter Lesevorgang kann abgehört und entschlüsselt werden. Zudem ist für die meisten Anwendungsfälle von RFID ein solcher Medienbruch nicht sinnvoll, da er den Einsatz von RFID sinnlos machen würde.

Ein weiteres Problem, das dem der Verschlüsselung der Datenkommunikation und der Autorisierung ähnlich ist, ist die Frage nach der Integrität der gespeicherten Daten. Der Proof-Of-Concept für einen RFID-Virus von

⁸ Eine Forschungsgruppe der ETH Zürich hat ein Konzept entwickelt, wie eine solche Autorisierungsüberprüfung in existierende RFID-Protokolle integriert werden können. Quelle; Floerkemeier, Schneider, Langheinrich: Supporting the Fair Information Practice Principles in RFID Protocols, 2004.

Weizenbaum⁹ zeigt, dass RFID-Systeme anfällig sind für die Manipulation von Daten. Zwar gibt es geeignete Gegenmaßnahmen wie Hash-Wertüberprüfungen, diese müssen aber auch implementiert sein, was heute nicht immer der Fall ist. Dass solche Datenmanipulationen nicht nur ein theoretisches Szenario sind, sondern mit einfachsten Mitteln durchführbar sind, zeigt das Open Source Programm RF-Dump¹⁰, das einem PDA ausgestattet mit einem handelsüblichen RFID-Transponder das Auslesen und Beschreiben von RFID-Chips ermöglicht.

Zusammenfassend kann gesagt werden, dass die heutigen RFID-Systeme nicht so sicher gegen Manipulation und Missbrauch sind, wie es für eine allgegenwärtige Technologie wünschenswert oder gar Bedingung ist, um ihr vertrauen zu können. Viele andere Nachteile, die gerne der RFID-Technologie angelastet werden, sind dagegen Kritiken an den Gesamtsystemen der Informationsverarbeitung, in denen RFID nur die unmittelbare Schnittstelle zu den Objekten darstellt.

9 siehe <<http://www.rfidvirus.org>>

10 siehe <<http://www.rf-dump.org>>

4.6 FRAGEN UND ANTWORTEN ZUR AUSWIRKUNG VON RFID

Abschließend sollen nun auch Fragen zum Thema RFID beantwortet werden. Diese sind sehr viel mehr meiner persönlichen Analyse entnommen als die Fragen und Antworten zu WMAN. Der Grund hierfür ist schlicht die Tatsache, dass RFID so kontrovers diskutiert wird und es zu einigen dieser Fragen frappierend unterschiedliche Antworten gibt. Am ehesten noch orientieren sich die hier gegebenen Antworten an den Überlegungen von Marc Langheinrich¹¹ und den Überlegungen im Buch »RFID – Applications, Security, and Privacy«, herausgegeben von Garfinkel/Rosenberg.

1. DÜRFEN DIE UNTERNEHMEN EIGENTLICH ALLES MIT RFID-TAGS VERSEHEN?

Ja, sie dürfen. Allerdings gibt es klare Richtlinien im Datenschutzgesetz, die dies reglementieren. So muss deutlich darauf hingewiesen werden, dass ein Produkt einen RFID-Chip trägt. Ebenso muss kenntlich gemacht werden, wo er sich befindet.¹² Zumindest in Deutschland und einigen anderen EU-Ländern ist die versteckte Anbringung von RFID-Chips nicht legal.

2. WIRD WIRKLICH ZUKÜNFTIG ALLES MIT EINEM RFID-LABEL VERSEHEN SEIN?

Die Vision des UC und insbesondere des Internets der Dinge sieht vor, dass alles miteinander kommunizieren kann. Alles mit RFID-Chips auszustatten, wäre der erste Schritt dahin. Aber schon heute zeigt sich, dass kaum jemand daran ein ernsthaftes Interesse hat. Der Wunsch, wirklich alle Dinge intelligent zu machen, scheint sich in Grenzen zu halten. Besonders hinsichtlich der Konsumprodukte des alltäglichen Gebrauchs scheint kaum ein Nutzen von einer Einzelidentifikation auszugehen. Der intelligente Kühlschrank wird sehr wahrscheinlich ein Konzept bleiben.

11 Marc Langheinrich arbeitet an der ETH Zürich im Bereich Computer Science mit dem Schwerpunkt Pervasive Computing und hat mehrere Dokumente zum Thema UC, RFID und Privatsphäre geschrieben oder war als Co-Autor tätig. Siehe <<http://www.inf.ethz.ch/personal/langhein/articles/>> und das Literaturverzeichnis.

12 siehe EICAR: Leitfaden RFID und Datenschutz, 2006-04-10 und BfDI: RFID – Funkchips für jede Gelegenheit?, 2004.

3. WIE KANN MAN SICH VOR UNGEWOLLTEM AUSLESEN DER CHIPS SCHÜTZEN?

Neben den in die Technologie integrierbaren Schutzmechanismen gibt es zwei Möglichkeiten, das ungewollte Auslesen zu verhindern. Einmal kann der RFID-Chip zerstört werden. Auf dem 22. Chaos Computer Congress wurde ein RFID-Zapper vorgestellt, der RFID-Chips zerstören kann, ohne das Trägermaterial zu verletzen.¹³ Andererseits kann man die Chips einfach abschirmen. Eine dünne Metallfolie genügt dafür. Für viele Anwendungen von RFID-Chips werden beide Lösungen nicht umsetzbar sein, aber für die im Alltag gebräuchlichsten schon.

4. IST RFID SCHON DAS INTERNET DER DINGE?

RFID ist ein integraler Bestandteil des Internets der Dinge, da es die Schnittstelle zwischen den Objekten und den ICT herstellt. Die momentan angedachten und existierenden RFID-Anwendungen sind aber vor allem als verbesserter Ersatz für andere Technologien zu sehen und sind als solche noch nicht als Internet der Dinge zu betrachten. Allerdings wird durch diese allmähliche Verbreitung von RFID die Grundlage für die Verbreitung der notwendigen Technologien für das Internet der Dinge vorangetrieben. Anwendungen wie das NFC-Mobiltelefon von Nokia, das für die mPayment-Lösung im RMV genutzt wird, werden dabei eine Vorreiterrolle spielen, um UCT im Alltag zu etablieren.¹⁴

5. WARUM IST DIE DISKUSSION UM RFID EIGENTLICH SO UNVERSÖNLICH?

Tatsächlich ist RFID eine sehr geeignete Technologie, um eine vollständige Überwachung und Kontrolle über die Vorgänge in einer Gesellschaft zu erreichen, und das sowohl durch Regierungen und Unternehmen als auch begrenzt von einzelnen Personen. Die Diskussion um RFID ist dabei viel eher als Stellvertreterkampf um Grundrechte wie Privatsphäre und informationelle Selbstbestimmung zu werten. RFID ist vor allem deswegen als Kampfplatz ausgesucht worden, weil diese Technologie so allgegenwärtig sein kann und wird. Letztendlich wird sich am Umgang mit dieser Technologie generell entscheiden, wie es um die Privatsphäre bestellt ist. Und da RFID sich gerade anschickt, weite Verbreitung zu finden, wird diese Diskussion so intensiv geführt. Es ist ein: »Wehret den Anfängen«, auch wenn es dafür eigentlich schon zu spät ist.

13 siehe <<https://events.ccc.de/congress/2005/wiki/RFID-Zapper>>

14 siehe <<http://rmvplus.de>> & <<http://www.europe.nokia.com/nokia/0,,55737,00.html>>

5 FÜNF-JAHRES-PROGNOSE

Eine zuverlässige Prognose für die sich so schnell wandelnde ICT-Landschaft und für die aufkommenden UCT zu treffen, ist nicht leicht und soll hier auch gar nicht geschehen. Aber zumindest können Tendenzen aufgezeigt werden, wie sich die Technologie und ihre Nutzung in den nächsten Jahren in Deutschland und anderen EU-Ländern entwickeln werden. Dabei ist ganz klar die massenhafte Alltagsnutzung gemeint und nicht die prinzipielle Existenz von Technologien und Anwendungen. Beispielsweise gibt es schon heute eine kleine Zahl von käuflichen Augmented Reality Anwendungen, diese sind aber noch nicht so beschaffen, dass sie eine bereitwillige massenhafte Nutzung erfahren könnten.

Im Wesentlichen soll hier eine Tendenz für die mobilen ICT im öffentlichen Raum aufgezeigt werden, wenn auch gerade diese Grenze zwischen mobil und fix, öffentlich und privat in den nächsten Jahren immer stärker verschwimmen wird. Die hier getroffenen Aussagen basieren auf vielen Dokumenten, etwa der OECD, ITU oder ISTAG, und vielen Nachrichten auf heise.de, slashdot.org, netstumbler.org und einigen weiteren technologiezentrierten Webseiten.

5.1 TENDENZEN FÜR RFID UND NFC

Für die nächsten Jahre wird es einen allmählichen Einzug von NFC-Systemen geben, die allerdings hauptsächlich als geschlossene Systeme auftreten werden und zur Authentifizierung und vor allem als schnelles Bezahlungssystem dienen werden. Systeme wie die Londoner Oyster Card werden eine sehr viel stärkere Verbreitung finden. So werden RFID-Smartcards Magnetstreifen- und Kontaktchipkarten weitestgehend ablösen. Darüber hinaus wird es vermehrt Testversuche mit RFID-getaggtten Werbemitteln geben, um zu sehen herauszufinden, wie solche Angebote aufgenommen werden. RFID-Systeme werden so allmählich in immer mehr Alltagssituationen Einlass finden. Dabei wird oft nicht von RFID, sondern von Smartcards, Smarts-hells oder eben NFC die Rede sein.

Konkurrenz zu den NFC-Systemen, die hauptsächlich für Bezahlvorgänge zum Einsatz kommen werden, wird das Mobiltelefon werden, das, mit entsprechender Software ausgestattet, heute schon in manchen Regionen als mPayment-Lösung eingesetzt wird.

RFID wird als Sicherungs- und Identifikationstechnologie für Tickets, wie sie etwa zur Fußball WM 2006 eingesetzt wurden, bei einer der nächsten Großveranstaltungen in die Kritik geraten, wenn Fälscher es geschafft haben werden, die RFID-Tickets zu kopieren und so ein totales Chaos beim Einlass verursachen.

Insgesamt wird sich RFID, ausgehend von den geschlossenen Anwendungsfällen, langsam im Alltag ausbreiten. Es wird auch Systeme geben, mit denen private Personen ihren Besitz selber mit RFID-Tags versehen können, um die bisher stummen Objekte in die fünfte Dimension zu holen.

5.2 TENDENZEN FÜR MOBILTELEFONE UND MOBILE COMPUTING

Das Mobiltelefon wird zur zentralen Anlaufstelle für alle Kommunikation unterwegs und wird noch mehr Dienste und Schnittstellen in sich vereinen. Die Geräteklasse der Smartphones/PDAs wird größere Verbreitung finden. Sie werden ausgerüstet sein mit GSM, UMTS, Wi-Fi, Bluetooth und RFID-Lesegerät. Wie es der UMA-Ansatz vorsieht, werden diese Geräte die Netze für die Telekommunikation beliebig wechseln können. Der Nutzer wird davon nichts merken. Gleichzeitig werden Dienste wie VoIP den klassischen Netzen immer mehr Nutzer abtrotzen. Besonders das GSM-Netz wird unter einer rapiden Abnahme der Teilnehmer leiden, wenn in den Ballungszentren VoIP-Dienste flächendeckend zur Verfügung stehen werden. Außerhalb der Ballungszentren wird es aber noch eine längere Zeit dauern, bis flächendeckendes WiMAX oder Wi-Fi zur Verfügung stehen wird. Es sei denn, es finden sich private Initiativen.

Insgesamt werden die Kosten für die Mobilfunkkommunikation weiter sinken. Wie heute schon bei den Festanschlüssen, wird die Zahl der Flatrates auch im mobilen Bereich erheblich steigen.

Um das Mobiltelefon herum werden die ersten ubiquitären Technologien entstehen, so wie heute schon die Zahl der Bluetooth-Headsets langsam, aber beständig zunimmt. Das Mobiltelefon als Schnittstelle zwischen WPAN und WAN/WMAN wird dabei noch auf längere Zeit eine wichtige Rolle spielen, auch wenn es in einer wachsenden Zahl von Anwendungen nur noch als Mittler aktiv sein wird. Die Serienreife von ePaper-Technologien wird eine ganze Reihe von neuen PDA-ähnlichen Geräten hervorbringen, insgesamt wird die Vielfalt der mobilen Computer dabei weiter zunehmen.

5.3 TENDENZEN FÜR DIE KONVERGENZ DER MEDIEN

Zunehmen wird die Zahl der Internetdienste, die auf eine mobile Nutzung ausgerichtet sind. Vor allem im Bereich Musik und Bewegtbild wird es viele Angebote geben, die sowohl den klassischen Rundfunkmedien als auch den MP3-Playern Konkurrenz machen werden.

Desweiteren wird es eine stärkere Verschmelzung von mobilen Diensten und fixen Diensten geben. Viele Dienste werden sich bemühen, ihr Angebot auf die mobile Nutzung auszudehnen. Vor allem die Community-Dienste und Portale werden versuchen, diese Möglichkeit zu ergreifen. Der dazu notwendige Schritt, immer mehr Informationen und Daten zentral auf Internetservern abzulegen, wird für immer mehr Bereiche erfolgen.

Auf der anderen Seite ist es durchaus möglich, dass mit der steigenden Zahl der Mobiltelefone, die mit offenen, also erweiterbaren Betriebssystemen ausgestattet sind, ein Virus oder ähnliche Schadsoftware sich über die bald allgegenwärtigen Bluetooth-Netze verbreiten und alles lahmlegen. Ein solcher Fall würde eine tiefgreifende Diskussion um die Sicherheit der Netze hervorrufen. Der Vertrauensverlust wäre gewaltig.

Darüber hinaus wird es in einigen Unternehmen oder Orten ein generelles Mobiltelefonverbot geben. Mit der Möglichkeit, schnelle Datenübertragungen zu vollziehen, stellen die zukünftigen WMANs und Endgeräte ein hohes Sicherheitsrisiko für Firmengeheimnisse dar. Es werden Möglichkeiten diskutiert werden, Mobiltelefone automatisch ausschalten zu können oder den Empfang effektiv zu stören.

5.4 TENDENZEN FÜR WEARABLES UND ÄHNLICHE UBIQUITÄRE TECHNOLOGIEN

Die nahtlose Integration von Technologie in Alltagsgegenstände wird in den nächsten Jahren in Form von Lifestyle-Produkten wie Nike+iPod¹ beginnen. Dabei wird Technologie noch immer als solche identifizierbar sein. Dennoch werden solche Partnerschaften wie im genannten Beispiel von Nike und Apple vermehrt stattfinden. Kleidung und Technologie nähern sich also gegenseitig. Echte Wearables, wo zwischen Kleidung und Technologie nicht mehr unterschieden werden kann, wird es erst in mehreren Jahren geben, also am Ende der hier betrachteten Fünf-Jahres-Spanne. Die ersten Einsatzgebiete werden Spezialanwendungen für Arbeitsbereiche sein, etwa dem Krankenhaus.

1 siehe <<http://www.apple.com/de/ipod/nike/>>

III. Umgang mit Technologien

1 DIE PRINZIPIELLE UNSICHERHEIT VON TECHNOLOGIE

Technologie ist dumm, denn sie ist weder lernfähig noch intelligent. Technologie folgt immer den ihr gegebenen Regeln. Zwar sind diese Regeln gerade bei ICT immer komplexer geworden, aber es bleiben feste Regeln. Es läuft immer auf die Überprüfung von Bedingungen hinaus, die ein eindeutiges »Ja« oder »Nein« erwarten. Kennt man diese Regeln gut genug, dann findet man auch Wege, sie zu umgehen. Will man also eine Technologie sicher machen, kann dies immer nur in einer Annäherung geschehen, die möglichst alle Nutzungsformen berücksichtigt. Sollen komplexe Aufgaben von der Technologie erledigt werden, also viele Nutzungen möglich sein, muss das Regelwerk, welche Arten der Nutzung legitim und welche es nicht sind, ebenso komplex sein. Je komplexer ein System wird, desto mehr Zwischenzustände kennt es und desto mehr Querverbindungen einzelner Subsysteme existieren. Diese Komplexität hat in Computersystemen ihren vorläufigen Höhepunkt gefunden. Ein modernes Betriebssystem besteht aus Millionen Zeilen Programmcode, um Funktionen vielfältigster Art bereitzustellen. Mit der Komplexität steigt aber auch die Gefahr, ungewollte Zusammenhänge und damit ungewollte Nutzungsmöglichkeiten zu übersehen. Je komplexer ein System wird, desto höher ist eine solche Fehlerwahrscheinlichkeit.

Für jeden Einsatz von Technologie sollte also immer mitbedacht werden, dass es niemals eine absolute Sicherheit geben kann, weder eine Sicherheit vor gewollter Manipulation von unauthorisierten Stellen noch vor der Disfunktion des Systems, wenn es vor vorher nicht bedachte Zustände gestellt ist.

Grundsätzlich kann Technologie relativ sehr sicher gemacht werden. Niemand käme auf die Idee, ein Auto vor jeder Fahrt auf volle Funktionsfähigkeit aller Teile zu überprüfen, sondern er vertraut darauf, dass Technik und Technologie funktionieren. Das Verhältnis zwischen der Dauer der Funktionalität und der Häufigkeit von Defekten oder Disfunktionen ist hinreichend bekannt, um dieses Vertrauen aufzubringen. Von einer solchen Sicherheit und Vertrauenswürdigkeit sind ICT-Systeme heute immer noch weit entfernt. Sie rechtfertigen in vielerlei Hinsicht noch nicht das Vertrauen, das ihnen entgegengebracht wird. Mit der immer stärkeren Verflechtung von ICT mit allen Bereichen in alle Bereiche des Lebens wird es umso wichtiger, dass sie so sicher werden, dass sie das Vertrauen rechtfertigen, auf dem eine selbstverständliche und beiläufige Nutzung basiert.

2 DAS ENDE DER LOKALEN DATEN

Die nächsten Jahre werden nicht nur eine Konzentration auf IP-basierte Netze bringen und damit die vielbeschworene Konvergenz der Medien, sondern die wachsende Zahl der schnellen Internetzugänge, ob nun mobil oder fix, wird auch die Art und Weise verändern, wo und wie Daten gespeichert werden. Als die Internetverbindungen noch sehr langsam waren, gab es eine klare Trennung von lokal gespeicherten Daten und auf Internetservern gespeicherten Daten. Das Internet war ein Ort speziell aufbereiteter Daten, die auf spezielle Art, als Webseiten, präsentiert wurden. Diese Aufbereitung war notwendig, damit die Informationen in akzeptabler Zeit übermittelt werden konnten. Seitdem aber immer schnellere Internetverbindungen zur Verfügung stehen, verändert sich die Nutzung des Internets. Es wird auch als Speicherort für nicht speziell aufbereitete Daten genutzt. Dieses Vorgehen hat eine Menge Vorteile, da die Daten an jedem Ort der Welt mit Internetzugang verfügbar sind und üblicherweise die Anbieter solcher Dienste auch professionelle Backup-Strategien fahren, sodass ein Datenverlust ohne Aufwand vermieden werden kann. Der Aufwand, selber lokal ein Backup der Daten vorzuhalten, entfällt. Genaugenommen entfällt sogar die Notwendigkeit, die Daten überhaupt lokal zu speichern.

Um die schnellen Internetzugänge und Speicherangebote haben sich in den letzten drei Jahren eine große Zahl verschiedenster Dienste entwickelt. Boten vor einigen Jahren Webmail-Dienste gerade genau diesen einen Dienst an, so scharft sich um den E-Mail-Account heute eine Vielzahl anderer komplexerer Angebote wie Adressbuch, Speicherplatz für allgemeine Daten, Fotogalerien, Gruppenverzeichnisse, Mailinglisten und vieles mehr. Ebenso gibt es Dienste wie »flickr« oder »youtube«, die sich auf die Katalogisierung und Distribution bestimmter Medien konzentrieren. Alle diese Dienste ergänzen dabei nicht nur lokale Anwendungen auf einem Computer, sondern ersetzen sie sogar und erweitern sie dabei gleichzeitig um die Möglichkeit der Veröffentlichung und Distribution.

Doch der Trend, immer mehr Anwendungen ins Internet auszulagern und den lokalen Rechner nur noch als Terminal zu nutzen wie in alten Mainframe-Zeiten, geht noch weiter. Nicht nur Google hat damit begonnen, auch klassische Officeanwendungen wie Textverarbeitung oder

Tabellenkalkulation als AJAX-Anwendung anzubieten. Damit verlagern sich auch Daten ins Internet, die man nicht unbedingt veröffentlichen will. Der Sinn, sie im Internet zu speichern, bleibt aber, kann man so doch jederzeit auf sie zugreifen, von wo auch immer. Daten und Anwendung sind immer verfügbar.

Diese Entwicklung, sowohl Daten als auch Anwendungen von einem Computer zu lösen und universell verfügbar zu machen, ist aber auch gleichzeitig eine Entfernung vom Computer an sich. Der Computer als zentrale Anlaufstelle wird in den kommenden Jahren an Bedeutung verlieren. Anwendungen werden auf den Geräten genutzt, die gerade zur Verfügung stehen. Mobil ist dies vielleicht ein Laptop oder ein ePaper-Computer oder Zuhause der Fernseher mit angeschlossener Spielkonsole. Die Internetanwendungen werden sich den Formfaktoren und Bedingungen automatisch anpassen und die Daten mediengerecht anbieten.

Diese Loslösung der Daten von lokalen Medien und einzelner Hardware ist damit ein wesentlicher Schritt zur Realisierung des Ubiquitous Computing, doch wirft sie auch Fragen auf.

Zwei wesentliche Fragen sind auch hier die nach Kontrolle und Sicherheit. Dienstanbieter wie Google, Yahoo oder Microsoft verlangen im Prinzip absolutes Vertrauen. Daten werden an Orten abgespeichert, auf die der Nutzer keinen Einfluss nehmen kann. Ebenso gibt es keinerlei Kontrollmöglichkeiten, ob der Dienstanbieter selber auf die Daten zugegriffen hat. Als Google seinen E-Mail-Dienst eröffnete, kündigten sie an, dass die gespeicherten E-Mails automatisch analysiert würden, um kontextsensitive Werbung einblenden zu können. Eine wochenlange Diskussion, ob ein solches Vorgehen sowohl legal als auch ethisch vertretbar sei, entbrannte daraufhin. Die Offenlegung dieser Vorgehensweise bescherte Google viel negative Presse, und das Firmencredo »Don't be evil« wurde das erste Mal öffentlich in Frage gestellt. Auch Googles Idee, dass E-Mails nicht mehr gelöscht werden müssen und deshalb auch in der Anfangsphase des Dienstes kein Löschen möglich war, wurde heiß diskutiert. Letztlich beugte sich Google und implementierte eine Löschfunktion. Die Idee, dass Google die gesamte E-Mail-Korrespondenz auf Jahre speichert und auswertet, war vielen dann doch zu unheimlich.

Dabei zeigt dieser Fall nur das generelle Problem, das allen Internetdiensten heute anhaftet. Man muss dem Betreiber glauben, rechtmäßig und richtig zu handeln. Ansonsten bleibt nur eine Nichtbenutzung der Dienste. Niemand kann überwachen, was die Betreiber innerhalb der Systeme tun. Die wesentliche Hoffnung besteht darin, dass sich kein Betreiber erlauben kann, solchen Missbrauch einer Allmachtposition zu betreiben, da ein Bekanntwerden katastrophale Folgen für das Unternehmen hätte.

Dass Misstrauen zum Misserfolg führen kann, musste vor allem Microsoft spüren, als sie den Passport-Dienst einführen wollten, der es ermöglichen sollte, verschiedene Dienste über eine Identität und damit auch nur ein Passwort zu nutzen. Vorgesehen war bei dem Konzept auch eine direkte Integration in das Betriebssystem, sodass zwischen lokalen Diensten und entfernten Diensten kein Unterschied mehr bestehen sollte. Dieses im Prinzip konsequente Vorgehen, dem Passwort und Sicherheitschaos zu begegnen, scheiterte schlicht daran, dass nur wenige bereit waren, Microsoft die Verwaltung anzuvertrauen und damit auch die Protokollierung aller Netzaktivitäten und mögliche Profilbildung zu ermöglichen.

Neben dem Problem der Kontrolle über den Umgang mit den entfernt gespeicherten Daten stellt sich aber auch die Frage nach der Integrität und Sicherheit dieser Dienste. Der Zugang zu diesen Diensten ist üblicherweise über einen Account geregelt, der Festlegung von Benutzernamen und Passwort erfordert. Bei vielen Diensten werden diese so wichtigen Daten zur Identifikation und Authentifikation im Klartext gesendet. Sichere Verbindungen für die Übertragung sind selten als Default, aber zumindest meistens als Option verfügbar. Neben dieser Missachtung grundsätzlicher Sicherungsmaßnahmen gegen das Abhören empfindlicher Daten bietet die Lösung aus Passwort und Name als Anmeldung jedoch auch deswegen nur mangelhaften Schutz, da die minimalen Vorgaben für die Länge eines Passworts meist immer noch nur 6 Zeichen sind, was eine Bruteforce- oder Wörterbuchattacke enorm vereinfacht. Dies geschieht immer mit dem Argument, dass sich niemand lange Passwörter merken kann und diese Vorgehensweise allemal besser sei, als sich ein langes Passwort aufzuschreiben.

Auch Dienste wie eBay gehen an diesen Stellen sehr fahrlässig mit der Sicherheit um. Da es bei eBay nicht nur um möglicherweise uninteressante private Daten geht, sondern um Geld, hat sich hier in der Vergangenheit schon öfter gezeigt, dass angelegte Nutzerkonten von Fremden gekapert und missbraucht wurden. Wie alle anderen Dienstanbieter arbeitet aber auch eBay nicht daran, das Anmeldeverfahren sicherer zu gestalten. Eine Verhaltensweise, die man etwa von einer Bank nicht akzeptieren würde.

Zusammengefasst bieten die bisherigen Gestaltungen der Internetdienste nicht die nötige Grundlage für das Vertrauen, das man jemandem gegenüber benötigt, um ihm oder einer Institution viele, vielleicht alle, persönlichen Daten anzuvertrauen.

3 DIE UNMÖGLICHKEIT VON FUNKTIONIERENDEM DIGITAL RIGHTS MANAGEMENT

In vielen Bereichen, die in dieser Arbeit angesprochen werden, taucht das grundlegende Problem der Kontrolle über Daten auf. Dieses Problem gründet aus der Freiheit der digitalen Daten von jedwedem Medium und ihrer beliebigen verlustfreien Duplizierbarkeit. Einer der Hauptansätze, um dieses Problem anzugehen, ist das Nicht-entstehen-lassen dieser Daten. Wo keine Daten erzeugt oder aufgezeichnet werden, können sie auch nicht missbraucht werden. Diesem Grundsatz folgen auch die Datenschutzgesetze etwa in Deutschland, die eine grundsätzliche Datensparsamkeit bestimmen. Doch dieser Ansatz ist nur in Maßen zukünftig anwendbar, da die kommenden UC- und ICT-Technologien darauf abzielen, Informationen zu erzeugen und zu verarbeiten.

Das Vorhandensein von Informationen muss also hingenommen werden und stellt gleichzeitig die Frage nach der Kontrollierbarkeit. Wie kann man Kontrolle über Informationen behalten, wenn andere Menschen, Organisationen oder Systeme darauf Zugriff haben?

Besonders aktiv mit diesem Problem haben sich in den letzten Jahren die Medienproduzenten auseinandergesetzt. Seit einigen Jahren wird erfolglos versucht, die Konsumenten in ihrem Umgang mit Filmen, Musik und anderen digitalen Medien zu kontrollieren beziehungsweise die Medieninhalte

auf vorgesehenen Gebrauch zu beschränken. DRM (Digital Rights Management) ist das Zauberwort. Doch die Wirkung des Zauberworts verpufft, denn wie bei jeder anderen Technologie ist es auch hier möglich, sie zu umgehen. Jeder neue Versuch der Medienproduzenten, mit neuen Technologien wieder Kontrolle zurückzuerlangen, wird über kurz oder lang durch Gegenmaßnahmen gekontert. Dass dabei noch nicht einmal die Verknüpfung von Inhalten an proprietäre Geräte nützt, zeigen die Spielkonsolen mit ihren eigentlich mächtigen DRM-Systemen und den Modifikations-Chips, die diese wieder aushebeln.

Jeder Versuch, ein technologiebasiertes System zu errichten, um die digitalen und damit anonymen Daten wieder identifizierbar zu machen und an Zugriffsberechtigte zu binden, scheitert. Technologie kann keine absolute Kontrolle bieten. Es gibt immer Möglichkeiten, Schutzmaßnahmen auszuhebeln, wenn auf Daten zugegriffen werden kann.

Die Anerkennung dieser Tatsache ist jedoch weder sonderlich bequem noch beliebt. Die jüngste Vergangenheit hat gezeigt, dass die Versuche, einen solchen Schutz doch zu realisieren, groteske Züge annimmt, die in der Sabotage von Computersystemen endet.¹ Der Versuch, den Nutzer der Daten, hier also den Konsumenten, zu entmündigen und in seinen Handlungsmöglichkeiten zu beschränken, hat etwa im Falle Sony-BMG zu einem tiefen Misstrauen geführt. Die technologische Reglementierung übersetzt sich für den Nutzer nämlich nicht nur in einer Entmachtung, sondern zeigt auch, dass ihm nicht vertraut wird. Und wer will mit jemandem kommunizieren oder Handel treiben, der offen zeigt, dass er einem misstraut?

Die negativen Effekte eines DRM sind, gesellschaftlich gesehen, somit möglicherweise noch wesentlich größer als oftmals gedacht wird. Denn das eigentliche Ziel, die Daten vor illegaler Verbreitung zu schützen, kann nicht erreicht werden. Die Wahl, die sich hier stellt, ist die zwischen beschränkter und vorgeschriebener, aber legaler Nutzung von Daten und Medien und der freien unbeschränkten Nutzung, die jedoch illegal ist, da die Beschaffungswege für »befreite« Daten meistens nicht legitim sind.

¹ Der wohl dramatischste Fall eines missglückten Kontrollversuchs, war ein Kopierschutz den Sony-BMG auf Musik-CDs einsetzte. Dieser installierte sich als Rootkit und bot nicht nur eine Angriffslücke für weitere Malware, sondern deaktivierte darüber hinaus auch bei manchen Rechnerkonfigurationen die Laufwerke.

Siehe <<http://www.heise.de/newsticker/meldung/73417>>

4 TRANSPARENZ

4.1 OPEN SOURCE VS CLOSED SOURCE

In den letzten Jahren ist auf breiter Front ein heftiger Streit in der Computerwelt entbrannt: auf der einen Seite die Verfechter der Closed Software, die fertige Softwareprodukte verkaufen wollen, und auf der anderen Seite die Open Source Gemeinde, die Transparenz und freie Nutzung von Software befürwortet. Eine wesentliche Frage ist hierbei wieder einmal die des Vertrauens. Bei Closed Source-Software ist man gezwungen, dem Anbieter zu trauen, dass die Software nur das tut, was sie soll. Im Gegenzug erhält man ein fertiges Produkt, um das sich vom Anbieter beschäftigte Entwickler kontinuierlich kümmern. Das Vertrauen in den Anbieter erstreckt sich dabei auch auf die Software, da man keine Möglichkeit hat, ihren Quellcode überprüfen zu lassen.

Auf der anderen Seite gibt es die Open Source-Bewegung, die nicht nur die Programme veröffentlicht, sondern auch den dazugehörigen Quellcode. Dies geschieht oft unter einer Lizenz, die es ermöglicht, auf Basis dieses Codes selber Veränderungen vorzunehmen oder den vorhandenen Code als Basis für andere Projekte zu nutzen. Dadurch, dass der Quellcode offenliegt, kann jederzeit von unabhängiger Stelle überprüft werden, was die fertige Anwendung tatsächlich tut.

Für ein grundlegendes Vertrauen in Technologie und ihre Anwendungen ist Transparenz notwendig. Bei Closed Source-Anwendungen ist dies in weiten Teilen ein blindes Vertrauen. Nur die Offenlegung des Quellcodes gibt die Möglichkeit, diesen zu überprüfen. Die in dieser Arbeit oft geforderte Transparenz kann also nur von Open Source Anwendungen erfüllt werden. Konzepte wie Shared Source, die Microsoft etwa forciert, um einem begrenzten Publikum einen begrenzten Zugang zum Quellcode zu gewähren, sind unter dem Aspekt der Transparenz nur bedingt hinreichend.

Konzepte, den Quellcode und die Funktionsweise durch Security by Obscurity zu schützen, wie sie etwa der Dienst Skype für seine Kommunikationsanwendung nutzt, ist dabei das genaue Gegenteil von Transparenz und im höchsten Maße bedenklich. Gerade das Beispiel Skype ist sehr bedenklich, da noch nicht einmal der Verschlüsselungsalgorithmus zur Überprüfung offengelegt wird.¹

1 siehe <<http://www.heise.de/newsticker/meldung/71094>>

Während Skype momentan extrem erfolgreich ist, obwohl keine Transparenz gegeben ist, zeigt sich an anderen Beispielen, dass gerade im Zusammenhang mit personenbezogenen Daten ein großes Misstrauen herrscht. Microsofts eigentlich sinnvoller Ansatz, mit dem Passport-Dienst eine zentrale Identitätsmanagement-Lösung anzubieten, scheiterte nicht zuletzt daran, dass die wenigsten Personen und Institutionen Microsoft vertrauten, mit den abgelegten Informationen im Sinne der Fair Information Practice umzugehen. Als dann noch Schwachstellen des Systems offenbar wurden, die die Sicherheit des Passport-Systems generell in Frage stellten, war es um Passport geschehen. Die Abhängigkeit der Online-Identität von einem Anbieter und einem geschlossenen System ist nicht akzeptabel. Neuere Ansätze, wie sie im Identitätsmanagement-Framework Bandit² Verwendung finden, sind nicht nur quelloffen, sondern belassen die Identitätsdaten unter der Nutzerkontrolle, auch was den Speicherort angeht.

4.2 TRUSTED PLATFORM MODULE

Unter einem vergleichbaren Vertrauensproblem, das auf mangelnder Transparenz basiert, leidet das Trusted Platform Module der TCG. Der eigentlich sinnvolle Ansatz, in jeden Computer oder jedes ähnlich arbeitende Gerät einen Chip einzubauen, der Verschlüsselung, Integritätsprüfung und DRM garantiert, stößt auf heftigen Widerstand, da das Design und damit die genaue Funktion des TPM nicht offengelegt wird³. Befürchtet wird, dass eine solche Blackbox im Computer dem Besitzer jederzeit die Kontrolle entziehen kann, wenn es dem Hersteller des TPM oder einem befreundeten Unternehmen beliebt.

Die Integration eines eigentlich wünschenswerten Chips, der nämlich tatsächlich eine hohe Manipulationssicherheit bietet, darf nicht dazu führen, dass der Besitzer eines Geräts nicht mehr die Kontrolle über dieses hat. Um die gewünschte Funktion zu gewährleisten und überprüfbar zu machen, muss ein solcher Chip vollständig in seiner Funktionsweise offengelegt werden und ebenso darf keine Möglichkeit besitzen, gegen den Willen des Besitzers eines Geräts zu agieren.

² siehe <http://www.bandit-project.org/index.php/Welcome_to_Bandit>

³ Das es auch anders gehen kann zeigt »Turaya«, eine OSS Trusted Computing Platform. Siehe <<http://www.heise.de/newsticker/meldung/74460>> und <<http://www.emsccb.de/content/pages/49373.htm>>. Turaya, ist aber noch im Entwicklungsstadium. 2006-06-22 erschien überhaupt die erste Demo-Version.

5 ANONYMITÄT, DATENSCHUTZ UND INTERNET

Wenn heute über Datenschutz im Internet oder Überwachung im Allgemeinen diskutiert wird, dann wird oft auf das Recht, anonym bleiben zu können, gepocht. Anonymität wird dabei oft synonym zu Privatsphäre verwendet. Dies ist in vielerlei Hinsicht für das Internet auch tatsächlich richtig. Bietet doch nur die Anonymität Schutz davor, dass profildbildende Daten aufgezeichnet, verarbeitet und mit einer Identität verknüpft werden können – ohne dass man weiß oder beeinflussen könnte, wer auf diese Daten Zugriff hat. Eine Bewegung im Netz verursacht immer eine Datenspur, die auf eine Identität zurückzuführen ist, wenn nicht Maßnahmen getroffen werden, diese Identität zu verschleiern. Durch die Möglichkeit, diese Spuren nicht nur im Moment zu verarbeiten, sondern sie ohne Limitierung zu speichern, können so an verschiedensten Stellen umfangreiche Bewegungsprofile erstellt werden. Die Konsequenz ist der totale Verlust von Privatsphäre, weil jede Handlung wahrgenommen und gespeichert wird. So ist die Unmöglichkeit der Identifikation für die Verfechter der Anonymität der einzige Weg, die Privatsphäre zu wahren. Anonymität ist gleichbedeutend mit Privatheit. Die Datensammelwut einiger Unternehmen oder staatlicher Institutionen, die dank lascherer Datenschutzgesetze in anderen Staaten als Deutschland sogar legitim ist, scheint den die Befürwortern eines Rechts auf Anonymität recht zu geben zu bestätigen.

Die Gegner von anonymer Nutzung des Internets dagegen predigen immer wieder, dass ein solch radikaler Datenschutz, der keine Identifikation zulässt, eigentlich immer nur Täterschutz sei. Wer nichts zu verbergen habe, brauche auch nichts zu befürchten. Eine Überwachung der Netzaktivitäten sei sinnvoll, um Straftaten aufzudecken. Die Verletzung der Privatsphäre sei ein akzeptables Übel. Dementprechend wird sogar oft ein Bann für Anonymisierungstechnologien gefordert.

Tatsächlich ist Anonymität ein Problem für die Integrität des Internets. Nur weil es überhaupt möglich ist, wirklich anonym zu bleiben, werden viele Straftaten nie aufgedeckt. Wenn etwa in einen Server oder Dienst unauthorisiert eingedrungen wurde, besteht keine Möglichkeit, den Täter zu finden.

Die permanente Überwachung aller Bewegungen im Internet, wie sie etwa die EU-Richtlinie zur Vorratsdatenspeicherung vorsieht, entspricht jedoch einer totalen Überwachung und dem völligen Verlust der Privatsphäre und ist somit unvereinbar mit rechtsstaatlichen Grundsätzen. Vereint man eine solche Überwachung des gesamten Telekommunikationsverkehrs noch mit der Vision des Ubiquitous Computing, entsteht ein totaler Überwachungsstaat.

Abgesehen von der Möglichkeit, eine permanente Überwachung zu etablieren, gibt es noch einen guten Grund gegen eine allgegenwärtige Datenspeicherung. Computersysteme sind nicht absolut sicher. Regelmäßig werden Fälle von Datendiebstahl bekannt. Mal sind es Kreditkartennummern, mal Sozialversicherungsnummern. Je mehr Daten aufgezeichnet werden, desto mehr potentielle Angriffsziele gibt es. Wo keine Daten gespeichert werden, können sie auch nicht in falsche Hände geraten.

Die Nutzung der ICT und vor allem der UCT darf nicht gleich einer totalen Überwachung sein. Die Nutzer dieser Technologien müssen darauf vertrauen können, dass ihr Recht auf Privatsphäre gewahrt bleibt. Gleichzeitig muss aber dennoch sichergestellt werden, dass dies nicht gleichbedeutend ist mit einer absoluten Anonymität, die als Deckmantel für Straftaten genutzt wird. In beiderlei Hinsicht darf die fünfte Dimension nicht zum rechtsfreien Raum werden.

6 PRIVATSPHÄRE IN ZWEI RICHTUNGEN

Privatsphäre ist das Recht, allein gelassen zu werden. Sie ist die Freiheit zu entscheiden, ob man kommunizieren möchte, was man kommunizieren möchte und mit wem. Diese Freiheit des Einzelnen, nicht zu kommunizieren, endet dort, wo Gemeinschaft existiert. Denn Gemeinschaft entsteht erst durch Kommunikation. Jede Gemeinschaft hat Regeln, die bestimmen, was kommuniziert werden muss, um an der Gemeinschaft teilzuhaben. Die Privatsphäre beschreibt also auch die Grenze zwischen Individuum und Gemeinschaft. Um die Freiheit zu haben zu wählen, wo diese Grenze liegt, und damit bestimmen zu können, in welcher Form der Einzelne sich in die Gesellschaft einbringt, muss der Einzelne Kontrolle über die Kommunikation haben.

Mit den Kommunikationsmedien verlagerte sich ein Teil der Kommunikation aus der unmittelbaren Kontrolle heraus. Das Ergebnis dieser langen Entwicklung sind die heutigen Kommunikationsmedien, die einen Großteil der Kommunikation vom Individuum unabhängig gemacht haben und einen völlig neuen Begriff der Gemeinschaft entstehen ließen. Eine Website mit persönlichen Mitteilungen kann von einer Milliarde Menschen empfangen werden. Ein riesiges Kommunikationssystem hat die ganze Welt greifbar nah werden lassen.

Die Gesellschaft ist in all ihren Zusammenhängen sehr komplex geworden, die Kommunikation ebenso. Ein gewöhnlicher Mensch hat heute Tausende Kommunikationspartner. Manche kennt er persönlich, manche treten als Institution in Erscheinung, manche bemerkt er gar nicht.

Viel dieser Informationsbereitstellung geschieht freiwillig, und in Anerkennung der gesellschaftlichen Regeln und aus dem Wunsch heraus, an der Gemeinschaft teilzunehmen. Einiges davon geschieht jedoch nicht freiwillig, und die Natur der gegenwärtigen Kommunikationstechnologien verhindert auch jegliche Kontrolle darüber. Einzig soziale Regeln verhindern heute, dass die Privatsphäre des Einzelnen fast völlig aufgehoben wird. Technologisch gesehen, ist es heute kein Problem, intimste Details weithin zu kommunizieren, wenn sie einmal bekannt sind.

Diese Möglichkeit der unbegrenzten Kommunikation ist heute noch limitiert auf die aktive und bewusste Nutzung von Technologien. Wir bemerken es noch, wenn wir Kommunikationstechnologien benutzen und Informationen über uns preisgeben, auch wenn wir danach nicht mehr wissen können, was damit geschieht. Mit der Vision der unsichtbaren Technologien, die uns allgegenwärtig umgeben und die selbstständig miteinander kommunizieren, droht aber auch dieser letzte Rest an Privatsphäre zu verschwinden. Wenn das Recht darauf, alleine gelassen zu werden, bewahrt werden soll, dann müssen Wege gefunden werden, diese feine Linie zwischen Individuum und Gemeinschaft auch in einem allgegenwärtigen Kommunikationsnetz zu ziehen.

Das Recht, allein gelassen zu werden, betrifft jedoch nicht nur die Kommunikation von innen nach außen, also die Entscheidung, welche Informationen das Individuum preisgeben möchte, sondern auch die Kommunikation von außen nach innen. Die Freiheit, keine Informationen bekommen zu wollen.

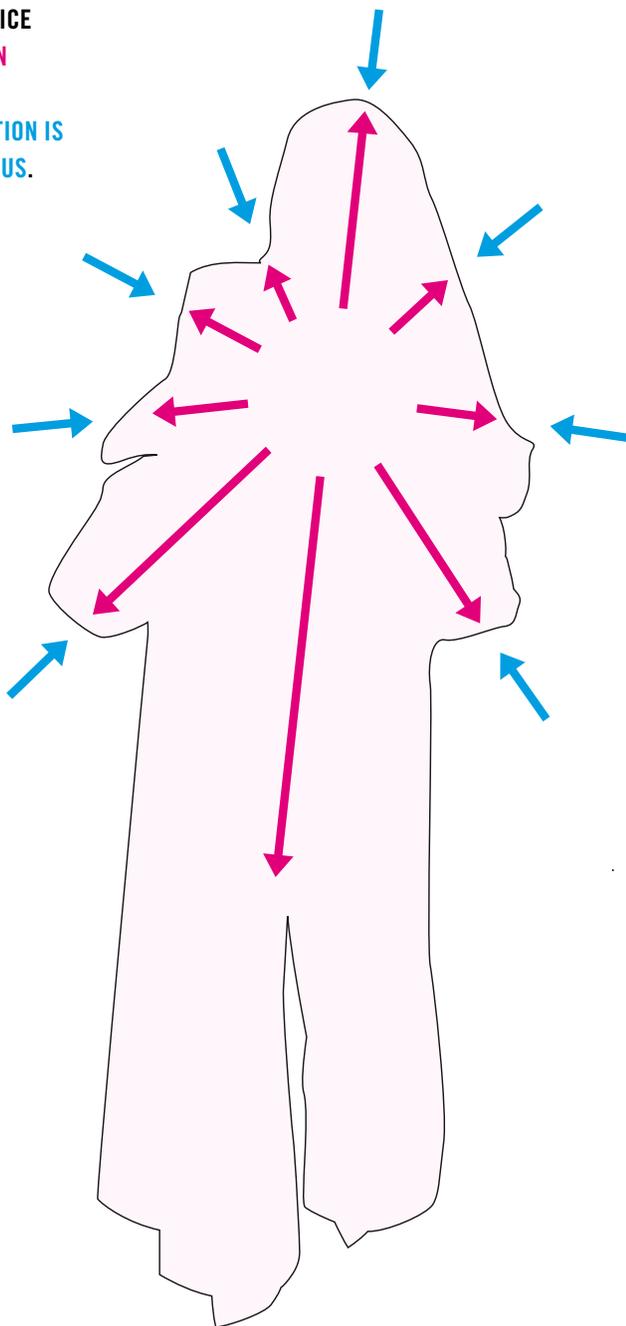
Heute ist dies noch kein großes Problem. Die Kommunikationsmedien können einfach ausgeschaltet werden, und wir sind nicht erreichbar. Wenn uns jemand auf der Straße anspricht, können wir einfach stumm weitergehen. Visuelle Kommunikation im öffentlichen Raum ist an Medien gebunden, auf die wir schauen können oder eben nicht. Wenn wir niemanden sprechen oder sehen wollen, dann gehen wir nach Hause, schließen die Tür ab und schalten alle Kommunikationsgeräte aus oder einfach nicht an.

Doch auch wenn wir kommunizieren wollen, mischt sich oft ungewollte Kommunikation dazwischen. Wir möchten E-Mail und SMS benutzen, aber sind verärgert über die ungewollten Werbebotschaften, die sich als Spam über uns ergießen. Dieses Problem wird sich potenzieren, wenn wir nicht mehr nur ein Mobiltelefon oder einen Computer besitzen, sondern unsere ganze Umgebung zum Kommunikationsmedium wird, wenn uns Hunderte von möglichen Kommunikationswegen umgeben.

Heute schon wird über die Informationsflut geklagt, die auf uns einstürzt, obwohl sie größtenteils nur passiv ist. Ein Wahrnehmungskollaps droht, wenn sie vollständig aktiv wird, wenn sich Botschaften von festen Orten und Medien lösen und uns permanent erreichen, über den gerade verfügbaren Weg. Für diese Problematik, wie wir zukünftig entscheiden können, welche Informationen uns erreichen, muss ein Weg gefunden werden. Das Recht, allein gelassen zu werden, muss weiterhin bestehen, auch wenn uns Kommunikationstechnologien vollständig und immer umgeben.

Wenn in dieser Arbeit die Privatsphäre vor allem im Kontext mit der Kommunikation nach außen betrachtet wird, dann liegt das vor allem daran, dass diese Richtung das sehr viel akutere Problem ist – es existiert nämlich bereits in sehr ausgewachsener Form. Implizit ist aber dennoch immer auch das Problem der Kommunikation nach innen mit vorhanden. Die Kommunikationsrichtung ist in vielen Fällen nicht entscheidend, sondern nur die Frage, wo und wie die Grenze gezogen wird.

**PRIVACY IS THE CHOICE
WHICH INFORMATION
IS PROVIDED AND
WHICH COMMUNICATION IS
ALLOWED TO REACH US.**



IV. Richtlinien für den Umgang mit Technologien

1 FAIR INFORMATION PRACTICE

Die Grundlage für viele Konzepte und Gesetze, die Privatsphäre und den Umgang mit personenbezogenen Daten angehend, ist die »Fair Information Practice« (FIP). Dieser Begriff wurde von der OECD in »Guidelines on the Protection of Privacy and Transborder Flows of Personal Data« geprägt, die erste Fassung wurde bereits 1981 veröffentlicht und 2002 grundlegend erweitert und komplettiert. Diese Richtlinien wurden damals erstellt, um bei der absehbaren Entwicklung von immer mehr personenbezogenen und elektronisch verarbeiteten Daten ein Grundgerüst zu haben, das die drei wesentlichen Ziele der OECD auch im Informationszeitalter schützen sollte. Diese drei Ziele sind pluralistische Demokratie, Achtung der Menschenrechte und freie Marktwirtschaft.

Obwohl bereits 1980 beschlossen, haben diese Richtlinien noch heute Gültigkeit, da sie nicht den Umgang mit Technologien als Ausgangspunkt haben, sondern den Umgang mit Daten im Allgemeinen. Auch die in der hier vorliegenden Arbeit beschriebenen Konzepte basieren auf den Grundprinzipien der FIP, da diese tatsächlich einen sehr ausgewogenen Ansatz zwischen Schutz der Privatsphäre und der informationellen Selbstbestimmung wie auch die Möglichkeit, Daten zu verarbeiten, bieten. In der Tat gehen die meisten Überlegungen und Arbeiten zu Datenschutz und Privatsphäre von der FIP aus. Aber hinsichtlich solcher Richtlinien, wie der in der EU beschlossenen Vorratsdatenspeicherung, kann nicht oft genug auf die Richtlinien der FIP hingewiesen und auf ihrer Anwendung beharrt werden. Die wichtigsten Richtlinien¹ werden wegen ihrer zentralen Bedeutung nicht nur für diese Arbeit nun zitiert:

COLLECTION LIMITATION PRINCIPLE

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

DATA QUALITY PRINCIPLE

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

¹ siehe S.14–16 in: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2002.

PURPOSE SPECIFICATION PRINCIPLE

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

USE LIMITATION PRINCIPLE

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

SECURITY SAFEGUARDS PRINCIPLE

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

OPENNESS PRINCIPLE

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

INDIVIDUAL PARTICIPATION PRINCIPLE

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him
 - i) within a reasonable time;
 - ii) at a charge, if any, that is not excessive;
 - iii) in a reasonable manner; and
 - iv) in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

ACCOUNTABILITY PRINCIPLE

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

2 TOWARDS A CULTURE OF SECURITY

Das Internet ist ein unsicheres Medium und ein gefährlicher Ort. Die existierenden Systeme und Strukturen waren primär dafür angedacht, das Internet als solches überhaupt erst einmal entstehen zu lassen. In der Euphorie über die Möglichkeiten des globalen Datenaustauschs wurden die Missbrauchspotentiale zwar erkannt, aber lange im Design der Systeme nicht als sonderlich relevant betrachtet. Die Systeme bauten auf dem Vertrauen auf, dass schon nichts passieren würde beziehungsweise die Missbräuche in der Summe nicht schwerwiegend sein würden.

Dass dies eine Fehleinschätzung war, ist heute längst bewiesen. Wer heute noch blind darauf vertraut, dass schon nichts passieren wird, wird sehr schnell eines Besseren belehrt – auf schmerzliche Art. Das Internet hat seine Unschuld verloren, ein generelles Misstrauen ist angebracht. Bestimmte Medien wie E-Mail trifft dies besonders hart. E-Mails sind so kompromittiert, dass viele Institutionen, wie Banken etwa, explizit darauf verzichten, E-Mails an ihre Kunden zu senden. Dem Kunden soll damit die Unsicherheit genommen werden, wenn er einschätzen soll, ob die E-Mail, die er gerade bekommen hat, tatsächlich von seiner Bank oder doch von einem Betrüger stammt. Solche Entscheidungen, auf E-Mail-Kommunikation zu verzichten, kommen einer Kapitulation gleich.

Das Problem der Vertrauenswürdigkeit und Sicherheit ist jedoch kein einfach zu lösendes Problem. Zu komplex ist das Internet geworden und zu eng sind viele Anwendungen und Systeme miteinander verwoben. Der Grundsatz, dass mit steigender Komplexität auch die Unsicherheit und die Fehlerwahrscheinlichkeit wachsen, trifft auf das Internet im Besonderen zu. Ein Fehler kann weltweite Auswirkungen haben. Die Ausnutzung von Sicherheitslücken in Clientsoftware hat dies bereits mehrfach unter Beweis gestellt. Malware wie der Wurm SQLSlammer, der 2003 große Teile des Internets lahmlegte und erst nach Tagen unter Kontrolle² zu bringen war, zeigten überdeutlich, wie anfällig das Internet heute ist und wie groß die Tragweite eines einzigen Fehlers sein kann. Das besonders Tragische an der SQLSlammer-Attacke war jedoch die Tatsache, dass bereits ein Patch existierte, um die vom Wurm genutzte Lücke zu schließen. Nur hatten Millionen von

2 siehe <<http://www.heise.de/newsticker/meldung/33987>>

Anwendern diesen Patch nicht installiert, aus Unwissen über die Notwendigkeit, die benutzte Software regelmäßig updaten zu müssen, oder aus Angst, dass nach einem Patch die Software nicht mehr funktioniert.³

Die Probleme liegen aber bei weitem nicht nur auf der Clientseite. Ein kompromittierter Server oder Serverdienst kann fatale Folgen haben. Als etwa in die Server des Debian-Projekts, einem Unix-Derivat, eingebrochen wurde, war erst nach einer längeren Untersuchung klar, dass die dort angebotene Software, insbesondere die Betriebssystemkernel, nicht verändert worden war. Hätte dies stattgefunden, wäre kompromittierte Software von ahnungslosen und gegenüber solchen Eingriffen machtlosen Nutzern heruntergeladen und eingesetzt worden.⁴

Die Liste der möglichen Angriffe ließe sich noch lange fortsetzen, aber schon die genannten Beispiele machen deutlich, dass das Internet in seinen heutigen Strukturen einer dringenden Reform bedarf, die über das Stopfen von Sicherheitslücken hinausgeht. Das Vertrauen in die Integrität des Internets ist bei denen, die sich mit der Problematik befassen, schon lange schwer angeknackst. Diejenigen, die das Internet heute noch sorglos nutzen, sind einfach nur nicht aufgeklärt.

Dieses berechtigte Misstrauen ist aber fatal für die weitere Entwicklung der Informationsgesellschaft. Auf einer so unsicheren Infrastruktur kann kaum eine Zusammenführung und Integration von immer mehr Systemen und Anwendungen des Alltags verantwortet werden. In den »OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security« wird diese Problematik thematisiert und Richtlinien für ein sicheres Internet, das unser Vertrauen wieder verdient, aufgestellt. Dabei wird auch klar herausgestellt, dass eine solche Reformierung des Internets eine gesamtgesellschaftliche Aufgabe ist.

3 Tatsächlich ist dies heute immer noch ein großes Problem. Regelmäßig treten nach Softwareupdates Probleme auf, die durch das Update verursacht werden. Dies hat dazu geführt, dass man heute wieder häufiger das alte Schlagwort »Never touch a running system« hört. Für Administratoren von Netzwerken und Netzdiensten wäre es sogar grob fahrlässig ein neues Patch oder Update ungeprüft auf ein Produktivsystem aufzuspielen ohne es vorher ausgiebig in Testsystemen auf Kompatibilität zu prüfen.

4 siehe <<http://www.heise.de/security/news/meldung/42565>>

Wie auch schon die Richtlinien zum Datenschutz sind hier die Formulierungen sehr allgemein und entsprechend weitreichend gefasst. Sie bieten eine sinnvolle Grundlage, für Sicherheitskonzepte von Netzwerken und Anwendungen und sollen auch für das hier vorliegende Konzept als Basis dienen. Die Zusammenfassung der Richtlinien⁵ lautet wie folgt:

1) AWARENESS

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

2) RESPONSIBILITY

All participants are responsible for the security of information systems and networks.

3) RESPONSE

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

4) ETHICS

Participants should respect the legitimate interests of others.

5) DEMOCRACY

The security of information systems and networks should be compatible with essential values of a democratic society.

6) RISK ASSESSMENT

Participants should conduct risk assessments.

7) SECURITY DESIGN AND IMPLEMENTATION

Participants should incorporate security as an essential element of information systems and networks.

⁵ siehe S.10–12 in OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002-07

8) SECURITY MANAGEMENT

Participants should adopt a comprehensive approach to security management.

9) REASSESSMENT

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

IN ALLER KÜRZE KÖNNEN DIESE RICHTLINIEN AUF EINE AUSSAGE GEBRACHT WERDEN:

»SECURE AND TRUSTWORTHY BY DEFAULT«.

3 RICHTLINIEN FÜR UBIQUITÄRE TECHNOLOGIEN

Die Richtlinien der beiden OECD-Dokumente sind richtigerweise sehr allgemein gehalten. Sie sind als allgemeine Entscheidungshilfen gedacht für den Einsatz und die Entwicklung von ICT-Systemen. Im Prinzip genügen sie schon als Grundlage für einen maßvollen und ethischen Einsatz von ICT. Für die im nächsten Kapitel folgenden Konzepte sind sie deshalb auch als wesentliche Grundlage genutzt worden.

Dennoch bedarf ein Konzept für den Umgang mit Ubiquitous Computing noch einiger weiterer Richtlinien, die speziell auf den Umstand eingehen, dass die kommenden Technologien für uns nicht mehr sichtbar sein werden. Die folgenden Richtlinien stellen somit eine Ergänzung zu den Richtlinien der beiden OECD-Dokumente dar.

1. TRANSPARENZ DER TECHNOLOGIE

Unsichtbare Technologien müssen auffindbar sein.

Die Idee des Ubiquitous Computing sieht vor, dass die Computersysteme und ihre Anwendungen sich unsichtbar in unseren Alltag integrieren. Unsichtbar darf jedoch nicht versteckt meinen. Versteckte Technologien sind in hohem Maße dazu geeignet, als Überwachungsinstrument für Unbefugte zu dienen. Technologie muss immer auffindbar und in ihren Strukturen begreifbar sein.

2. ENTSCHEIDUNGSFREIHEIT DER NUTZUNG

Technologie muss ausschaltbar sein.

Genauso wie Technologie auffindbar bleiben muss, muss auch die Entscheidungsfreiheit bestehen bleiben, sie zu nutzen oder nicht. Wenn eine Nutzung nicht erwünscht ist, muss die Möglichkeit gegeben sein, den Dienst oder das Gerät vollständig zu deaktivieren.

3. TRANSPARENZ DER KOMMUNIKATION

Kommunikation muss nachvollziehbar sein.

Es muss für einen Beteiligten jederzeit feststellbar sein, welche Kommunikationen stattfinden oder stattgefunden haben, bei denen personenbezogene Informationen übermittelt wurden. Dies beinhaltet auch eine eindeutige Identifizierbarkeit der Kommunikationspartner. Versteckte Kommunikation ist in hohem Maße dazu geeignet, als Überwachungsinstrument für Unbefugte zu dienen. Die Dauer der Aufzeichnung muss dabei so limitiert sein, dass sie es nicht ermöglicht, als Überwachung zu fungieren.

4. BEGRENZUNG DER KOMMUNIKATION

Die Reichweite der Übertragung muss auf das notwendige Maß minimiert sein.

Als wesentliche Sicherheitsschwachstelle des UC ist die Funkübertragung erkannt worden, die grundsätzlich ein hohes Angriffspotential bietet. Um dieses Risiko zu minimieren, ist eine Limitierung der Sendereichweite auf das notwendige Maß unbedingt erforderlich.

5. VERSCHLÜSSELUNG DER KOMMUNIKATION

Es dürfen keine unverschlüsselten Daten übertragen werden.

Die Verschlüsselung der Kommunikation ist unabdingbar, um funktionierende Sicherheits- und Authentifizierungskonzepte zu implementieren. *Diese Richtlinie ist eigentlich schon durch die OECD-Richtlinien abgedeckt, sie ist aber so essentiell für die Integrität der Kommunikation, dass sie hier noch einmal explizit aufgeführt ist.*

V. Das Privatsphärenmodell

Im Anschluss an die Betrachtungen über Technologie und ihre Nutzung und welche Richtlinien dabei möglichst beachtet werden sollen, soll nun ein Konzept folgen, wie es möglich sein könnte, auch im Falle von Kommunikation die Wahl zu haben, wie weit diese Kommunikation gehen darf beziehungsweise wo die Grenze liegt, die als Privatsphäre bezeichnet werden kann. Wie schon festgestellt, kann nicht wirklich effektiv verhindert werden, dass Informationen beliebig genutzt werden, wenn sie einmal zugänglich gemacht wurden. Ein Modell zum Schutz der Privatsphäre muss also von dem Vertrauen ausgehen, dass ein Kommunikationspartner mit den ihm gegebenen Informationen nicht gegen uns handelt. Effektives und vor allem absolutes Digital Rights Management ist nicht möglich.

Es kann bei einem solchen Privatsphärenschutz also immer in erster Linie nur darum gehen, welche Informationen preisgegeben werden und wie dies reglementiert werden kann. Dieser Ansatz ermöglicht dabei im Umkehrschluss auch den Schutz der Privatsphäre in der Kommunikation von außen nach innen, wenn man auch bestimmen kann, welche Informationen in die Privatsphäre eindringen dürfen.

1 GRUNDLAGEN UND REGELN

1.1 PRIVATSPHÄRE VS KOMMUNIKATION

Bevor nun im Folgenden das Konzept für die Privatsphäre in der fünften Dimension erläutert wird, muss erst noch einmal die logische Struktur der Privatsphäre geklärt werden, da dies bisher noch nicht geschehen ist, auch wenn ständig von ihr die Rede war. Man kann die Privatsphäre sinnbildlich als begrenzten Raum verstehen, der angefüllt ist mit der Identität und dem Wesen der Person – und zwar in allen fünf Dimensionen. Außerhalb dieses begrenzten Raums ist offener, unbegrenzter Raum – die Öffentlichkeit. In diesem offenen Raum bewegen sich nun alle Personen und kommunizieren. Jede Kommunikation ist dabei immer auch ein gegenseitiges Eindringen in die Privatsphäre. Je nachdem, wie viele und welche Informationen über die Identität und das Wesen der Personen ausgetauscht werden, umso stärker ist das Eindringen.

Um dieses Eindringen kontrollieren zu können, haben sich komplexe soziale Kommunikationsmechanismen entwickelt, die insbesondere als Kategorisierung der Kommunikationsfälle dienen. Dem langjährigen Freund wird ein anderer Status und Zugang zu Informationen gewährt als einem vorbeilaufenden Unbekannten.

Die Preisgabe von personenbezogenen Informationen geschieht immer auf gegenseitigem Vertrauen. Sind sich die Kommunikationspartner unbekannt, gilt dabei, dass der Initiator der Kommunikation auch als erster seine Identität preisgibt. Dieser Vertrauensvorschuss ermöglicht überhaupt erst die Kommunikation. Generell kann gesagt werden, dass vertrauensschaffende Informationen auch immer identitätsbildende Informationen sind. Je mehr man jemandem vertraut, desto mehr Informationen über die Identität wird man preisgeben, was bei einer Gegenseitigkeit zu immer mehr Vertrauen führt. Zusammengefasst lassen sich über die Privatsphäre und die Kommunikation folgende Feststellungen treffen, die sich dann im Folgenden auch auf die Kommunikationsmedien übertragen lassen:

1. Nur die Nichtkommunikation gewährleistet eine unangetastete Privatsphäre.
2. Wer kommuniziert, gibt einen Teil seiner Identität und Privatsphäre preis.
3. Der Initiator einer Kommunikation muss damit beginnen, sich zu identifizieren.
4. Je privater und umfangreicher die Informationen sind, umso größer muss das Vertrauen sein.
5. Vertrauen aufbauen ist ein komplexer Prozess, der hohe Investitionen erfordert, an Zeit, Aufwand oder identitätsbildenden Informationen.
6. Je weniger personenbezogen eine Information ist, desto weniger Vertrauen wird benötigt, um sie zu kommunizieren.
7. Nur anonyme Informationen werden auch anonym kommuniziert.

1.2 PRIVATSPHÄRE ALS SUMME DES BESITZES

Da sich UCT im Gegensatz zu den heutigen Technologien auch mit dem uns umgebenden Raum verbinden sollen und werden, ist es auch notwendig, diesen Aspekt zu betrachten. Privatsphäre im Raum definiert sich vor allem über Besitz- und Kontrollrechte. Eine Wohnung darf nur mit Erlaubnis des Bewohners betreten werden – sie ist Privatsphäre. Ebenso gilt dies für jeden anderen Besitz. Die Erlaubnis, mit dem Mobiltelefon eines anderen telefonieren zu dürfen, muss erst eingeholt werden, bevor telefoniert werden darf. Eben solcher Regeln bedarf es auch für die Definition von Privatsphäre in UC-Systemen. Die Besitz- und Kontrollrechte der physischen Welt müssen sich auch in der Kommunikationsebene abbilden lassen. Der Besitzer entscheidet, welche Form der Kommunikation zulässig ist. Der Besitzer muss dabei für ein Gerät identifizierbar sein, aber dieses Besitztum muss nicht zwangsläufig anderen Personen mitgeteilt werden. Daraus resultiert eine Privatsphäre als geschlossenes Netzwerk der Geräte, das sich um die Identität des Besitzers formt.

1.3 ANONYMITÄT IM ÖFFENTLICHEN NETZ

Die meisten Dienste oder Informationen sind heute im Internet frei verfügbar. Eine Identifikation des Nutzers ist nicht notwendig – und sollte deswegen auch nicht geschehen. Um ein Netzwerk aufzubauen, bedarf es aber immer einer Identifikation der Sende- und der Empfangsstationen, um Daten überhaupt austauschen zu können. Für die gegenwärtigen Computernetzwerke ist dies meist die IP-Adresse.

Um eine dauerhafte Identifikation des Nutzers über die IP-Adresse zu verhindern, die es etwa auch ermöglichen würde, eine Standortbestimmung im realen Raum durchzuführen, wenn ein Fixpunkt bekannt ist, muss diese IP-Adresse zufällig bestimmt und damit dynamisch sein. Erst durch einen ständigen Wechsel der IP-Adresse und eine nicht nachvollziehbare Zuordnung des Nutzers zu der IP-Adresse kann eine dauerhafte Überwachung oder Profilbildung vermieden werden.

Vorteilhafterweise muss in ad-hoc- Netzwerken eine solche IP-Adresse unbedingt dynamisch vergeben werden, sie muss einzigartig sein, um Adresskollisionen zu vermeiden. Die technische Notwendigkeit könnte als Anonymisierung instrumentalisiert werden, indem etwa regelmäßig auch ohne technischen Zwang die IP-Adresse geändert wird.

Generell gilt also der Grundsatz, dass ein offener Dienst auch anonym genutzt werden können muss. Wer als Betreiber die Identität eines Nutzers kennen möchte, muss den Dienst vor der anonymen Nutzung schützen, etwa durch Anmeldungszwang oder durch die Privatsphärenpräferenzen – zu diesen später mehr.

1.4 GESCHLOSSEN UND DOCH OFFEN

Die gegenwärtigen Wi-Fi-Netzwerke schützen sich vor dem Eindringen unbekannter Geräte durch einfache Regeln. Entweder ein Gerät kennt das Passwort, oder es erlangt keinen Zugang. Hat es Zugang, kann es vollwertig mit den anderen Netzteilnehmern kommunizieren. Die zukünftigen Netze sollen sich aber selbstständig im ad-hoc-Verfahren bilden können. Da gerade im WPAN keinerlei Infrastruktur vorhanden sein wird, sondern die Endgeräte selber zu Vermittlungsstellen werden, ist es unerlässlich, dass sie diese Funktion auch ausführen können. Ein solcher Weiterleitungsdienst muss also immer verfügbar bleiben, selbst wenn ein Objekt andere Dienste nur autorisierten Geräten zur Verfügung stellt. Ein Gerät muss also abbilden können, dass es Teil eines geschlossenen Privatsphärennetzes und gleichzeitig Teil eines offenen Netzes sein kann.

1.5 VERSCHLÜSSELUNG

Um die Trennung eines geschlossenen Netzwerks vom einem offenen Netzwerk überhaupt zu ermöglichen, muss der Datenverkehr im geschlossenen Netz verschlüsselt vonstatten gehen. Nur so kann sichergestellt sein, dass zwar die Route der Daten beliebig und frei ist, aber der Inhalt des Datenverkehrs dennoch nur von den gewollten Kommunikationspartnern verstanden wird. Die Verwendung von asymmetrischen Verschlüsselungskonzepten bietet sich hier sehr an.

1.6 IDENTITÄTSMANAGEMENT

Die Privatsphäre ist eng verknüpft mit der Identität. Eine Person wird dabei von einem Panoptikum von Identitäten umgeben. Je nach Kontext bilden unterschiedliche und unterschiedlich viele Informationen die Identität. Auch in der fünften Dimension haben Personen eine Fülle von Identitäten. Diese zu verwalten, bedarf es einer umfassenden Lösung, um nicht den Überblick zu verlieren; sind doch mit diesen Identitäten oft auch Rechte verbunden, wie der Zugang zu bestimmten Diensten.

Was heute noch hauptsächlich Dienste betrifft, wird in Zukunft auch Objekte und Orte betreffen, die ebenso eine Identität haben müssen, und die wiederum ebenso verwaltet sein muss, um etwa den Besitz und damit die Kontrolle definieren zu können.

Desweiteren gilt es, nicht nur die eigenen Identitäten zu verwalten, sondern auch die anderer Personen und die Rechte, die man diesen Personen zubilligen will. Die Vergabe der Rechte haben Instant Messaging Dienste bereits mit der Vergabe der Kontaktliste verbunden. Eine solche Lösung muss es für alle Repräsentationen in der fünften Dimension geben, um eine Privatsphäre definieren zu können.

1.7 EINFACHHEIT ODER »PRIVACY BY DEFAULT«

Eine der wesentlichen Forderungen an ein solches Privatsphärenmodell ist die Einfachheit der Handhabung. Es bedarf heute einer Menge Fachwissen, Erfahrung und stetiger Recherche, um einen Computer oder ein Computernetzwerk abzusichern. In der ubiquitären Zukunft wird aber alles vernetzt sein und sich viele Teilnetze, Objekte und Dienste unter der Kontrolle und Verantwortlichkeit von völlig unerfahrenen und unwissenden Benutzern liegen. Sicherheit und damit auch Privatsphäre müssen aber einfach zu erreichen sein können – es darf nicht sein, dass jeder Nutzer zu einem Netzwerkadministrator heutiger Art werden muss.

Als Ansatz sollte daher gelten, dass Objekte und Dienste per Voreinstellung so agieren, dass sie die Privatsphäre des Nutzers oder der besitzenden Person wahren. Erst die willentliche Bekundung, die Privatsphäre einzuschränken, darf zu einer Öffnung führen. Ebenso darf die Verwaltung der Privatsphäre, so komplex die Mechanismen dafür sind, nicht kompliziert sein. Sie muss selbstverständlicher Teil der Nutzung von Technologien sein und nicht aufgepfropft und umständlich.

2 IDENTITÄTEN

2.1 DIE KERNIDENTITÄT

Um eine Privatsphäre festlegen zu können, muss sie einen zentralen Punkt haben – die Person selber. Für die Privatsphäre in der Infosphäre gilt dasselbe, eine Person benötigt eine Repräsentanz, um die herum die Privatsphäre entstehen kann. Diese Repräsentanz soll hier Kernidentität genannt werden. Die Kernidentität beinhaltet Informationen, die sie eindeutig mit einer Person verknüpfen. Dementsprechend darf auch nur diese Person Zugang zu dieser Kernidentität besitzen, denn die Kernidentität gewährt auch Zugang zur Summe aller personenbezogenen Informationen und Identitäten, die eine Person um sich herum vereint. Die Kernidentität entspricht somit einem Hauptschlüssel, der Zugang zu einem Schlüsselbund gewährt, der Schlüssel zu allen Diensten, Daten und Identitäten enthält. Ein bekanntes Prinzip, das heute schon etwa in MacOS X Anwendung findet und für viele Identitätsmanagement-Lösungen grundlegend ist. Zugleich ist die Kernidentität aber auch Abfragestelle für Anfragen nach der Authorisation beim Zugriff von Identitäten auf Dienste oder Objekte.

Um die Sicherheit und Verfügbarkeit der Kernidentität zu gewährleisten müssen einige Regeln unbedingt eingehalten werden. Die Kernidentität darf nicht permanent an ein physikalisches Objekt gebunden sein. Ein Verlust oder die Disfunktion des Objekts würde sonst dazu führen, dass die so zentrale Kernidentität nicht mehr verfügbar ist, oder wenn auch geschützt in die Hände Fremder gelangen kann.

Ebenso muss sichergestellt sein, dass die Kernidentität wirklich an die Person gebunden ist, zu der sie gehört. Um dies zu erreichen, ist eine physikalische Authorisation zwingende Voraussetzung. Dies könnte anhand von über die Eingabe einer PIN über ein TUI geschehen, oder über den Abgleich biometrischer Daten wie den Fingerabdruck oder DNS-Scan.

Die Personenbindung der Kernidentität ist also essentiell. Als weitere Regel zur Erhöhung der Sicherheit und Personenzentrierung muss feststehen, dass die Eingabe und Bedienung über ein zuvor autorisiertes TUI immer eine höhere Befehlsgewalt hat, als telekommunikative Befehle oder Voreinstellungen. Diese Regel ist auch notwendig, um sicherzustellen, dass die Person volle Kontrolle hat, und nicht andere Personen oder Institutionen.

2.2 IDENTITÄTEN

Identitäten sind Informationen, die eine Kommunikation ermöglichen beziehungsweise die Nutzung eines Dienstes. Beispiele sind die Telefonnummer, die E-Mail-Adresse oder Benutzername und Passwort für den Zugang zu einer Webseite. Mit den identitätsbildenden Daten werden auch Metadaten zum Dienst abgespeichert, die ihn charakterisieren, etwa die Privatsphärenpräferenzen oder die zugehörigen Dienstklassen, siehe unten.

Allgemein wichtig ist jedoch, dass eine Identität keine Rückschlüsse oder Zugriffsmöglichkeiten auf alle Identitäten gewähren darf. Dieses Recht muss der Kernidentität vorbehalten sein. Um dies zu verhindern, darf eine Identität niemals automatisiert angelegt werden, sondern bedarf der Interaktion der Kernidentität und damit der einzigen autorisierten Person.

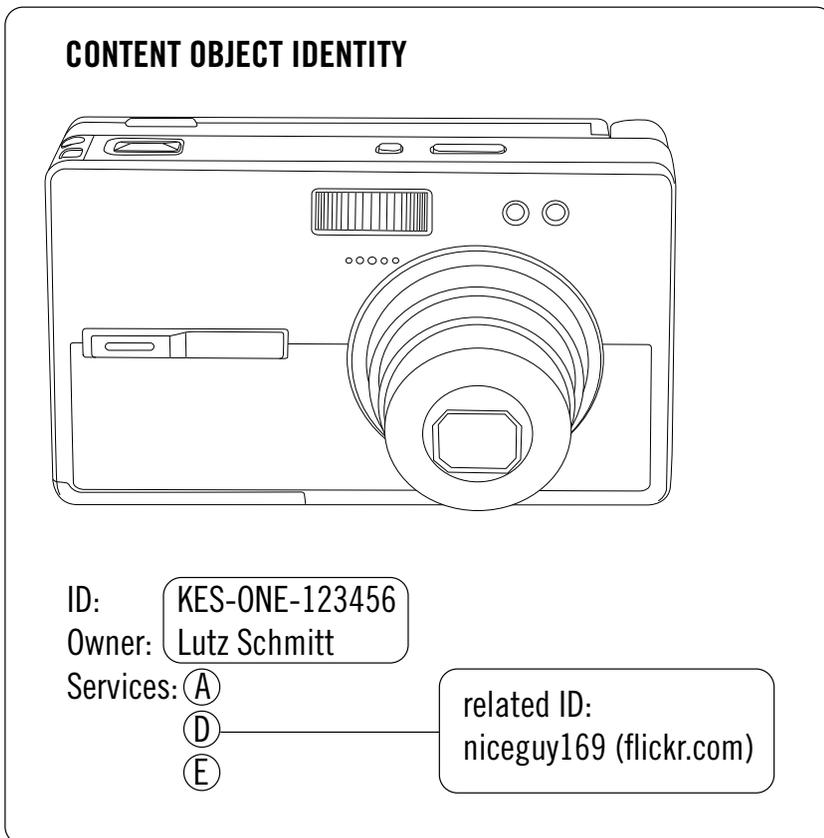
2.3 OBJEKTIDENTITÄTEN

Objektidentitäten sind fest im Objekt verankert. Sie ermöglichen eine allgemeine Identifikation eines Objekts gegenüber der Kernidentität. Sie enthält dafür Informationen zu den Kommunikationsschnittstellen des Objekts und den angebotenen Diensten, falls diese fest angelegt sind. Neben diesen Informationen enthält die Objektidentität eine eindeutige einmalige Identifikationsmöglichkeit entsprechend einer Seriennummer beziehungsweise EAN-Code. Üblicherweise wird diese Nummer errechenbar sein und ist deswegen nicht geeignet, als Schlüssel zur Bindung an die Kernidentität zu dienen.

Gelangt ein Objekt durch eine Transaktion in den Besitz einer Person und damit in deren Privatsphäre, wird in deren Kernidentität eine aus Sicht der Person lokale Objektidentität für dieses Objekt angelegt, die die Informationen der Objektidentität abbildet und um die Besitzeridentität ergänzt. Diese Information über den Besitzer muss auch im Objekt abgelegt werden. Damit können sich Kernidentität und Objekt jederzeit eindeutig gegenseitig identifizieren. Ebenso muss das Objekt nicht selber Identitäten Zugangsberechtigter verwalten, sondern kann diese Informationen jederzeit abrufen ohne eine Interaktion der Person.

Einem Objekt können mehrere Identitäten zugesprochen werden, etwa von verschiedenen Personen, um diesen die Nutzung der Dienste des Objekts und die Speicherung von Daten im Objekt zu ermöglichen. Ein Objekt kann aber nur einen Besitzer haben, der damit die Rolle des Administrators übernimmt.

Dadurch, dass die Objektidentität an eine Person gebunden ist, muss sie nicht extra verwaltet werden, sondern kann als Untermenge der Kernidentität verwaltet werden.



2.4 ORTSIDENTITÄTEN

Diese Klasse ist genau genommen nur eine erweiterte Objektidentität. Zu den Identitätsmerkmalen der Objektidentität kann bei Orten oder fest verorteten Objekten die geographische Lage als zusätzliches Identifikationsmerkmal dienen. So lassen sich auch ganze Räume als Privatsphäre definieren, etwa Hotelzimmer oder die eigene Wohnung. Es lassen sich aber auch Regeln aufstellen, an welchen Orten welche Kommunikation legitim ist.

2.5 FREMDIDENTITÄTEN

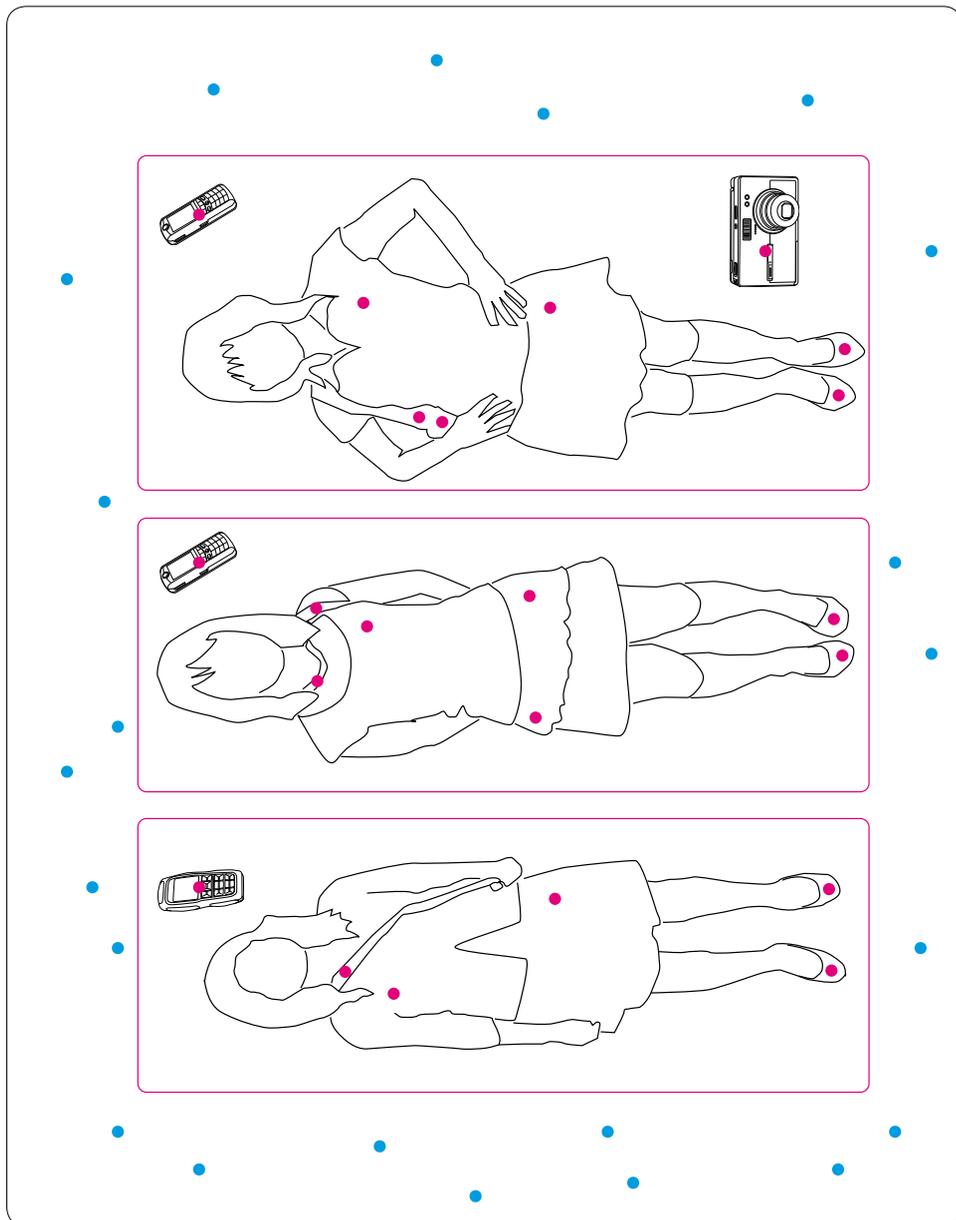
Die Summe der Fremdidentitäten ist im Prinzip nichts anderes als ein Adressbuch. Um eine Identität, die einer Person, einem Unternehmen oder einer Institution entsprechen kann, gruppieren sich die Kontaktdaten und andere personenbezogene Informationen. Ebenso können hier Nutzungsrechte für Objekte beziehungsweise Diensten zugeteilt werden. Dies geschieht am einfachsten durch Gruppen, kann aber auch einzeln geschehen.

2.6 OVERVIEW OF THE IDENTITIES AND THEIR CONTENTS

The colors are indicating the default location in the privacy spheres.
 For identities the default location depends on the service class.

CORE IDENTITY	IDENTITY	FOREIGN IDENTITY
all identities	service class identifier	unique user identities
all object identities	service metadata	service metadata
all foreign identities	unique user identity	personal metadata
unique personal identity	access to service	information about related
all personal information	personal metadata	foreign object identities and location identities
OBJECT IDENTITY	LOCATION IDENTITY	
unique identifier	STRUCTURAL	
ownership identifier	all contents an object identity	
information about identities for provided services	can contain geographic metadata	
	GROUP BASED	
	information about contained (object) identities	
	geographic metadata	

DISTINCTION BETWEEN PERSON AND PUBLIC THROUGH OWNAGE



3 SCHICHTEN DES PRIVATSPHÄRENMODELLS

Aus dieser Identitätenstruktur ergeben sich drei Schichten. Die persönliche Schicht der eigenen Identitäten und Objektidentitäten, die private Schicht der bekannten Fremdentitäten und die öffentliche Schicht, die alle unbekannt Fremdentitäten enthält. Diese Schichten können schon als einfaches Regelwerk für die Kommunikationsbereitschaft verwendet werden, deren drei Zustände so aussehen:

1. ÖFFENTLICH

Abfragen und Kommunikation sind von jeder Person und jedem Objekt möglich. Es wird aktiv nach Kommunikationspartnern gesucht.

2. PRIVAT

Nur bekannte Fremdentitäten dürfen kommunizieren und Informationen abfragen beziehungsweise erhalten aktiv Statusinformationen. Unbekannte Anfragen werden abgeblockt.

3. PERSÖNLICH

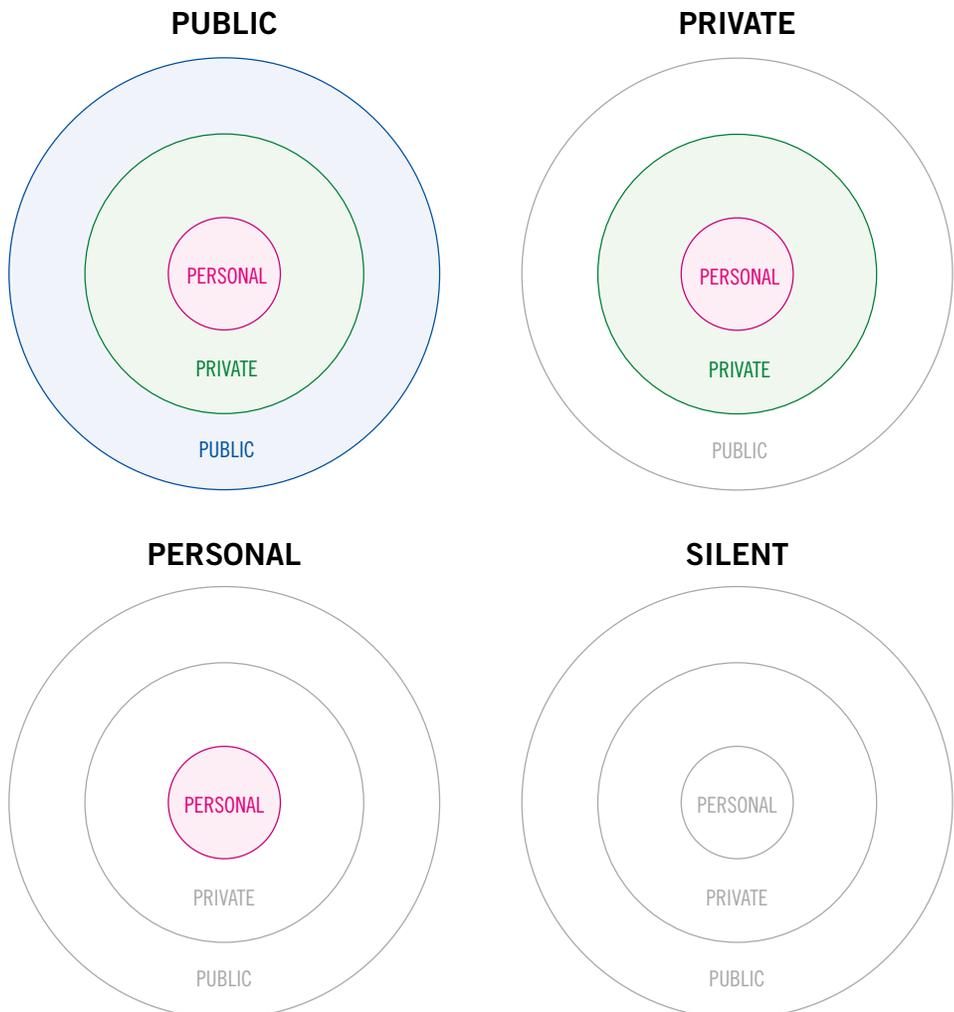
Kommunikation findet nur innerhalb der eigenen Identitäten statt. Alle anderen Kommunikationsanfragen werden abgeblockt.

Um der Forderung zu entsprechen, dass Technologien vollständig deaktiviert werden können, bietet es sich an noch eine weitere Schicht »Stumm« einzuführen. Sie ist das Äquivalent zum Ausschaltknopf, den viele Objekte zukünftig garnicht mehr haben werden. Ein Dienst oder Objekt, das auf »Stumm« gesetzt ist, wird erst durch Aufforderung einer autorisierten Identität wieder aktiv. Zur Vereinfachung und weil es für die Erhaltung der Privatsphäre ausreichend ist, wenn Dienste oder Objekte auf Persönlich gesetzt werden, wird diese unterste Sphäre nicht weiter behandelt.

Die drei Sphären ermöglichen eine Zuordnung von Diensten und Kontakten, und durch die Kommunikationslimitierung auf eine niedrigere Sphäre den Ausschluß von bestimmten Diensten und Nutzern. Möchte man etwa von niemandem angerufen oder lokalisiert oder anderes werden, stellt man die Privatsphäre auf »persönlich« ein. Jeder Dienst und damit verbundene Fremdentitäten, die in einer höheren Schicht verortet sind, werden abgeblockt. Ist die Einstellung auf »öffentlich«, wird jede Kommunikation

zugelassen. Dies bedeutet aber nicht automatisch, dass die Schichten durchdrungen werden. Auch wenn die allgemeine Einstellung auf »öffentlich« steht, werden Dienste der persönlichen Schicht auch nur in der persönlichen Schicht verfügbar sein. Es ist aber durchaus möglich, durch Nutzerinteraktion einen Dienst oder ein Objekt in eine höhere Schicht zu heben. Um diese Verwaltung der Schichten möglichst einfach zu halten, ist eine Klassifizierung der Dienste und die Möglichkeit, Gruppen zu bilden, notwendig.

BASIC COMMUNICATION SETTINGS OF THE PRIVACY SPHERES



4 DIENSTKLASSEN

Um die Bildung der drei Schichten automatisiert vornehmen zu können, müssen entfernte Dienste wie auch von Objekten angebotene Dienste klassifiziert werden, sodass sie per Voreinstellung einer Schicht zugeordnet werden können. Die hier vorgenommene Klassifizierung ist auf die Anwendung im Privatsphärenmodell abgestimmt, es ist aber durchaus denkbar, diese Klassifizierung zu verfeinern, um auch für andere Anwendungsfälle dienen zu können. Für das Privatsphärenmodell sind jedoch nur folgende Klassen notwendig:

A IDENTIFIKATIONSDIENSTE

Identifikationsdienste bedienen die Kommunikation der Identität. Diesen Dienst bieten alle Dienste und Objekte an, in manchen Fällen, wie einfachen RFID-Chips, ausschließlich.

B LOKALISATIONSDIENSTE

Genaugenommen ist ein Objekt, sobald es kommuniziert, auch lokalisierbar. Da aber möglicherweise Kommunikationsbereitschaft besteht, aber nicht der Wille, den Ort preiszugeben, muss die Verortung gesondert behandelt werden.

C KOMMUNIKATIONSDIENSTE

Hierunter fallen alle Dienste, die in irgendeiner Form zur Kommunikation zwischen Personen geeignet sind.

D PUBLIKATIONSDIENSTE

Publikationsdienste sind Dienste, die es ermöglichen, im Kontext des Dienstes gespeicherte oder erzeugte Daten anzubieten.

E INFORMATIONSGEWINNUNGSDIENSTE

Hierunter fallen alle Dienste, die Informationen aus den Messdaten von Sensoren erzeugen. Dies können die unterschiedlichsten Daten sein: Ton, Bild, Film, Bewegung, medizinische Daten.

Diese Klassen können einmalig einer Schicht zugeordnet werden und verbleiben auch in dieser, falls dies nicht manuell geändert wird. Werden zum Beispiel die Identifikationsdienste in die persönliche Schicht eingeordnet, stehen solche Dienste nur noch dort zur Verfügung. Mit einer solchen Einstellung würden etwa alle RFID-Tags, die in den Besitz einer Person gelangen, sofort unsichtbar für den Rest der Welt.

Durch die Klassifizierung der Dienste und nicht der Objekte wird es auch möglich, dass ein Objekt mehrere Dienste unterschiedlicher Verortung in den Schichten in sich vereint, aber dennoch die Privatsphäreinteilung erhalten bleibt. Beispielsweise könnte eine Kamera zwar ihre Identität nicht der Öffentlichkeit preisgeben, aber dennoch automatisch die geschossenen Bilder mithilfe eines entsprechenden Dienstes veröffentlichen.

Die Zuteilung der Klassen kann dabei nach persönlichen Präferenzen geschehen. Um einen hohen Schutz der Privatsphäre zu gewährleisten, müsste sie allerdings so aussehen:

Öffentlich: –

Privat: C

Persönlich: A, B, D und E

Die Klassen dienen dabei der Vereinfachung der Kontrolle über die Privatsphäre. Es ist immer möglich, auch einzelne Dienste entgegen der Voreinstellung in eine andere Sphäre zu heben.

5 GRUPPIERUNGEN UND ABHÄNGIGKEITEN

5.1 MANUELLE GRUPPEN

Die hier aufgezeigte automatische oder per einmaliger Voreinstellung vorgenommene Schichtung und Steuerung der Privatsphäre hat jedoch Grenzen. Gerade die Schicht »Privat« benötigt feinere Einteilungen, um dem Wunsch nach Privatsphäre nachkommen zu können, ohne dabei unter ungewollten Limitierungen zu leiden.

Um dies zu erreichen, können Identitäten so gruppiert werden, sodass sie voneinander unterscheidbar werden. Diese Gruppen müssen allerdings vom Nutzer vorgegeben werden. Ob eine Fremdidentität einem Freund, einem Geschäftskontakt oder einem Familienmitglied gehört, kann nicht sicher automatisch festgestellt werden. Mit solchen Gruppierungen ist es auch möglich, Dienste und Identitäten unterschiedlicher Schichten zusammenzufassen. Beispielsweise möchte man vielleicht für Freunde in der Mittagspause lokalisierbar sein, um gemeinsam zu essen, dies aber anderen bekannten oder gar unbekanntem Fremdidentitäten nicht ermöglichen.

Wie komplex diese Gruppen werden und wie viele es sind, ist jedem Nutzer selbst überlassen. Die Anzahl wird sich aus einer Abwägung zwischen dem Wunsch nach Privatsphäre und dem Wunsch nach Einfachheit der Bedienung ergeben. Ein gangbarer Weg zur Vereinfachung der Verwaltung ist die Hierarchisierung der Gruppen, die deshalb möglich sein muss.

Mittels zusätzlicher Metadaten zu (Fremd-)Identitäten lassen sich zudem Regeln anlegen, die zu einer automatischen Gruppenbildung führen. Diese Metadaten müssen dafür aber zur Verfügung stehen, was nicht unbedingt gegeben ist, sodass ein solcher Automatismus Grenzen hat beziehungsweise manueller Pflege bedarf.

5.2 AUTOMATISCHE HIERARCHIEN UND OBJEKTABHÄNGIGKEITEN

Um zu vermeiden, dass Objekte nicht genutzt werden können, falls einmal der Zugang zur Kernidentität nicht möglich sein sollte, können die zum Objekt gehörigen Identitäten, also Objektidentität und Identitäten der angebotenen Dienste, auch im Objekt gespeichert werden. Die lokale Anmeldung am Gerät geschieht dann über die Geräteidentität, die dann auch gleichzeitig alle Dienste freischalten kann. Diese Form der Kopplung von Identitäten an Objekte entspricht der gegenwärtigen Situation.

Darüber hinaus ist es möglich, Objektidentitäten miteinander zu verknüpfen beziehungsweise unterzuordnen. Dies kann automatisch geschehen, wenn das Objekt, über das diese Einstellungen lokal vorgenommen werden, immer als übergeordnete Instanz gesehen wird. Das bediente Objekt speichert dafür auch die Objektidentitäten der anderen Objekte.

Auf diese Weise ist es möglich, ohne Zugang zur Kernidentität eine teilfunktionale Privatsphäre aufzubauen. Beim nächsten Einloggen mit der Kernidentität können die Änderungen übernommen werden, sodass es nie zu einer Diskrepanz zwischen Daten in der Kernidentität und in den Objekten kommt. Aber auch mit Zugang zur Kernidentität ist die Zentrierung der Privatsphäre um das Objekt, das gerade lokal bedient wird, wichtig, da sich der Nutzer dort befindet. Auf diese Weise entstehen selbstständig Hierarchien und Subsysteme. Objekte ohne HCI werden dabei immer in die Abhängigkeit von Objekten geraten, die eine direkte Nutzerinteraktion ermöglichen.

Eine solche Hierarchisierung ermöglicht auch eine Verwaltung getrennter Subsysteme. Alleine durch die Steuerung über ein und dasselbe Interface werden diese Gruppen dabei gebildet. Diese können institutionalisiert werden, um geschlossene Gruppen zu bilden und so für unterschiedliche Orte und damit verbundene Objekte und Dienste unterschiedliche Einstellungen für die Privatsphäre vorzunehmen. Die eigene Wohnung oder der Arbeitsplatz wären Beispiele für solche Subsysteme.

6 ZUSÄTZLICHE FILTER UND KONTROLLMÖGLICHKEITEN

6.1 LOCATION BASED FILTERS

Ausgehend und ergänzend zu dem Privatsphärenmodell ergeben sich viele Möglichkeiten für UC-Anwendungen, wenn man die geographische Verortung mit einbezieht. Am ehesten lassen sich diese Konzepte mit Location Based Filters umschreiben. Im Gegensatz zu den momentan aufkommenden Location Based Services geht es dabei nicht darum, Dienste anzubieten, sondern Kommunikation zu kontrollieren.

Dafür ist es allerdings zwingend erforderlich, dass ein Ort auch in der fünften Dimension repräsentiert wird durch eine Ortsidentität. Falls eine solche nicht existiert, könnte auch über die Objektidentitäten indirekt eine Ortsidentität definiert werden, indem man Objektidentitäten gruppiert und diese Gruppe manuell mit geographischen und beschreibenden Metadaten versieht.

Begibt man sich an einen so definierten Ort, können zusätzliche Regeln angewendet werden, die Kommunikation erlauben oder verbieten. Beispielsweise kann festgelegt werden, dass ein Sensor, der Körperfunktionen überwacht, nur dann diese Daten außerhalb der persönlichen Sphäre übermittelt, wenn er an einem Ort ist, an dem dies gestattet ist. Auf der Straße ist es ihm verboten, aber im Behandlungszimmer des Arztes sehr wohl erlaubt und sogar erwünscht.

Weitere mögliche Filterregeln könnten auch die Entfernung von Besitzer beziehungsweise kontrollierendem Objekt und abhängigem Objekt sein. Ein Mobiltelefon, welches abgelegt wird, könnte sich automatisch sperren, oder, wenn es einer anderen Person übergeben wird, temporär die Identität der Person annehmen, die es gerade hält, damit diese damit telefonieren kann, und zwar mit ihren Identitäten.

Denkbar wäre auch die automatische Stummschaltung der Objekte, wenn bestimmte Räume wie Besprechungszimmer betreten werden, sodass nicht vergessen werden kann, die Kommunikationsgeräte auszuschalten, und eine störungsfreie Besprechung möglich ist.

6.2 TIME BASED FILTERS

Wendet man nicht nur Ortsidentitäten als Filter an, sondern nutzt auch Uhrzeit oder Datum als Filterregel, steigt die Zahl der möglichen Voreinstellungen noch einmal erheblich. Zeitbezogene Regeln können vor allem helfen, Kommunikation mit anderen Personen oder Personengruppen auf ein gewünschtes Maß zu reduzieren. Nach Feierabend darf der Arbeitgeber nur noch auf die Mailbox sprechen. Denkbar wäre auch eine Kombination von zeit- und ortsbezogenen Filterregeln. Auch hier bleibt es wieder der Person überlassen, wie komplex diese Filterregeln werden.

6.3 SPY CONTROL

Die Privatsphäre ist zukünftig nicht nur dadurch verletzlich, dass ungewollte Kommunikation aus der Entfernung stattfinden kann. RFID-Chips und ähnliche Technologien werden so klein und unauffällig, dass sie im Prinzip überall untergebracht werden können. Es kann davon ausgegangen werden, dass bei geschäftlichen Transaktionen darauf hingewiesen wird oder nach geltendem Datenschutzgesetz sogar darauf hingewiesen werden muss, dass erworbene Objekte Funktechnologien enthalten. Es sind aber durchaus Szenarien denkbar, bei denen die Anbringung oder Übergabe solcher funkenden Objekte nicht bemerkt oder nicht kenntlich gemacht wird. Im Ergebnis würde unbewusst ein offen funkender Chip an der Person getragen und so mindestens die Bewegungen im Raum verfolgbar werden. Wenn weitere Sensoren integriert sind, würden sogar noch mehr personenbezogene Daten an Unbekannte übermittelt werden.

Um solche Szenarien zu erschweren oder gar vollständig zu verhindern, muss eine regelmäßige Überprüfung der eine Person umgebenden Objekte beziehungsweise Dienste erfolgen. Wird dabei etwa festgestellt, dass ein unbekanntes Objekt dauerhaft anwesend ist, dann kann ein Alarm erfolgen. Die eigenen Objekte und Dienste können in so einem Fall eine schnelle Ortung durch Funkpeilung ermöglichen. Ein solches Szenario ist unter Berücksichtigung der sehr geringen Investitionskosten für eine solche Überwachung nicht allzu unrealistisch.

Probleme könnte eine solche Maßnahme gegen Überwachung in dichten Menschenmengen machen, da es nicht unwahrscheinlich ist, dass sich andere Menschen samt ihrer Privatsphäre und den darin enthaltenen Diensten parallel zu einer Person bewegen. Es muss eine geeignete Eingrenzung solcher Kontrollen auf den extremen Nahbereich des Körpers erfolgen beziehungsweise auf die unter der Kontrolle stehenden Systeme, das Auto etwa. Ein häufiger Fehlalarm könnte dazu führen, dass das System abgeschaltet wird. beziehungsweise zu Verfolgungswahn verschiedenster Ausprägung führen könnte. Ein solches Kontrollsystem sollte dazu dienen, dass man der Technologie vertrauen kann, und nicht gegenteilige Gefühle erzeugen. Dass ein solches Kontrollsystem jedoch wünschenswert oder gar notwendig ist, trotz der möglichen Schwierigkeiten bei der Realisierung, zeigt etwa eine TAUCIS-Studie¹. Der Gedanke an unkontrollierbare Überwachung weckt viele Bedenken gegenüber den kommenden UCT.

¹ siehe TAUCIS: Auswirkungen des Ubiquitous Computing (UC) auf Verbraucher: Chancen und Risiken, 2006-03.

7 PRIVATSPHÄRE WÄHREND DER KOMMUNIKATION

7.1 PRIVATSPHÄRENPRÄFERENZEN

Die bislang definierten Funktionen und Regeln des Privatsphärenmodells ermöglichen detailliert eine Unterscheidung zwischen gewollter und ungewollter Kommunikation. Doch auch während der Kommunikation oder Nutzung von Diensten muss eine einfache Möglichkeit zur Definition und zum Schutz der Privatsphäre gewährleistet sein.

Besucht man etwa ein Internetangebot, fällt innerhalb dieses Dienstes eine große Menge an Daten an, die, verknüpft mit einer Identität und der Speicherung dieser Daten, zu einem sehr komplexen Nutzungsprofil führen. Dies kommt einer permanenten Überwachung gleich. Nach gegenwärtigen Datenschutzrichtlinien muss man solchem Vorgehen zustimmen. Diese Zustimmung geschieht heute jedoch sehr pauschal. Zwar gibt es Maßnahmen, um eine Verknüpfung vieler Daten mit einer Identität zu verhindern, aber dafür ist einiges an Wissen notwendig. Wenn man sich nicht aktiv schützt, verliert man jede Privatsphäre.

Eine Lösung hierfür sind die Privatsphärenpräferenzen, die einmalig abgeleget werden und die akzeptierten Regeln für den Umgang mit personenbezogenen Daten enthalten. Eine solche Regelung legt auch der Dienst an. Will man nun einen Dienst benutzen, werden die eigenen Privatsphärenpräferenzen mit denen des Dienstes verglichen. Halten sich die Bedingungen des Dienstes im Rahmen der eigenen Präferenzen, kann der Dienst ohne weiteres genutzt werden. Will der Dienst mehr oder auf andere Art Daten erheben und verarbeiten, muss der Nutzer dem zustimmen. Lehnt er ab, kann er den Dienst oder die betroffenen Teile des Dienstes nicht nutzen. Stimmt er zu, weiß er, inwiefern seine Privatsphäre beeinträchtigt wird. Diese Lösung entspricht dem Grundsatz »Privacy by default«. Die Voreinstellungen müssen dabei noch nicht einmal besonders detailliert sein:

1. AUTOMATISCHER LOGIN

Wenn im eigenen Schlüsselbund eine Identität für diesen Dienst vorhanden ist, soll der Nutzer mit diesem automatisch angemeldet werden?

2. IDENTITÄTSBINDUNG

Dürfen die bei der Nutzung eines Dienstes automatisch anfallenden Daten mit einer beim Dienstleister verbleibenden Identität verknüpft werden?

3. AUSWERTUNG

Dürfen die freiwillig angegebenen Daten personenbezogen, anonymisiert oder gar nicht für Zwecke verwendet werden, die über die notwendige Verarbeitung im Rahmen der Dienstleistung hinausgehen?

4. ZEITRAUM DER SPEICHERUNG

Neben den Daten, die notwendig sind, um den Dienst zu nutzen, und deshalb dauerhaft gespeichert sind, fallen noch viele weitere Daten an. Wie lange dürfen diese gespeichert werden?

5. WEITERGABE VON DATEN AN DRITTE

Einige Daten müssen zur Ausführung der angebotenen Dienste an Dritte weitergegeben werden. Dürfen darüber hinaus weitere personenbezogene Daten an Dritte weitergegeben werden?

Diese fünf Regeln genügen schon, um die Privatsphäre weitreichend zu schützen, wenn dem Kommunikationspartner vertraut wird. In ihrem striktesten Fall gewähren sie eine bis auf die IP-Adresse anonyme Nutzung eines Dienstes.

7.2 REDUZIERUNG DER NOTWENDIGEN DATEN

Viele Angebote im Internet, insbesondere denen die, bei denen wo es zu Geld- und Warentransaktionen kommt, benötigen heute zur Durchführung dieser Dienstleistungen viele personenbezogene Daten, von der Kontonummer bis zur Adresse. Andere Dienste sichern sich durch Überprüfung angegebener Daten ab, dass eine Person auch tatsächlich die ist, für die sie sich ausgibt, um einen Missbrauch des Dienstes ahnden zu können. Nach der Übermittlung solcher Daten muss der Nutzer dem Unternehmen vertrauen, dass es die Daten nicht nur gegen unerlaubten Zugriff schützt, und ebenso dass es sie auch nicht aktiv in unerlaubter Weise weitergibt.

Um das Risiko des Auftretens solcher Fälle zu minimieren, ist die einfachste Lösung, solche Daten nicht zu übermitteln. Hierfür kann die Kernidentität als Signatur dienen beziehungsweise mit ihr eine glaubwürdige Identität gegenüber dem Dienst erzeugt werden. So kann eine sichere Identifikation einer Person vorgenommen werden, ohne dass weitere Daten übermittelt werden müssen.

Am Beispiel einer Warenbestellung über das Internet lässt sich dies gut darstellen. Anhand der sicheren Identität, die ein Nutzer angelegt hat, wird eine Vorgangsnummer erzeugt. Diese Nummer wird sowohl dem Lieferanten als auch dem Nutzer übermittelt, der ebenso die Kontaktdaten des Lieferanten erhält.

Der Nutzer übermittelt nun diese Vorgangsnummer samt Aufforderung, das Geld zu übermitteln, an seine Bank. Ebenso sendet er seine Lieferadresse an den Lieferanten. Ist das Geld von der Bank angewiesen, gibt der Internetanbieter die Ware frei und sie wird zugestellt. Bei dem gesamten Vorgang wurde an personenbezogenen Daten einzig und allein die Lieferadresse versendet, und auch die nur an die notwendige Stelle.

Ein solches System funktioniert selbstverständlich nur, wenn alle Stellen mit Identitätssignaturen umgehen können und entsprechende Kommunikationskanäle aufgebaut sind.

8 SCHWACHSTELLEN

8.1 VERFÜGBARKEIT DER KERNIDENTITÄT

Eine wesentliche Grundvoraussetzung für das vollständige Funktionieren des Privatsphärenmodells ist die Verfügbarkeit der Kernidentität. Sie ist zentraler Anlaufpunkt zur Verwaltung, aber auch für die automatisierte Rückfrage von Identitäten nach Berechtigungen. Damit sie wirklich immer verfügbar ist, muss sie ausfallsicher aufbewahrt werden. Eine Speicherung auf eigenen Geräten ist letztlich zu unsicher. Schon ein Stromausfall oder ein leerer Akku genügen, um den Zugang zur Kernidentität zu verhindern. Noch katastrophaler wären der Verlust oder ein Totalschaden des Geräts, auf dem die Kernidentität gespeichert ist. Einen ausreichenden Schutz gegen Ausfall und Verlust können eigentlich nur Data-Center gewährleisten. Die Speicherung und die Verfügbarhaltung der Daten sind das Kapital der Betreiber der Data-Center. Dementsprechend gut sind die Schutzmaßnahmen.

Die Idee, die eigene Identität in die Obhut eines gewinnorientierten Unternehmens zu geben, weckt jedoch Bedenken. Eine sinnvolle Möglichkeit scheint eine gemeinnützige Organisation als Betreiber eines solchen Dienstes. Dabei müssten Wege gefunden werden, diese Organisation zu finanzieren, ohne in Abhängigkeiten zu geraten. Denn die Bereitstellung der Kernidentität darf nichts kosten – Geld darf kein Kriterium sein, ob man sich ein funktionierendes System zum Schutz der Privatsphäre leisten kann.

Eine weitere Lösung wäre die Ablage der Kernidentität auf vielen Geräten, möglicherweise sogar fremden. Da sie ohnehin nur stark verschlüsselt abgelegt wird, wäre dies ein gangbarer Weg, der aber das erhöhte Risiko in sich birgt, dass die Verschlüsselung gebrochen wird, weil auf die Daten selbst zugegriffen werden kann. Für ein Funktionieren des Privatsphärenmodells ist die Lösung dieses Problems essentiell.

8.2 ANONYME ÜBERGABE VON BESITZ- UND KONTROLLRECHTEN

Bei der Übergabe von Besitz- und Kontrollrechten darf kein Besitzvakuum entstehen, das einer Identitätsungebundenheit entspricht. Eine solche Lücke würde es Angreifern ermöglichen, Besitz zu ergreifen. Vertrauen sich die beiden Transaktionspartner und kennen sie sich, ist dies kein Problem. Das Besitzrecht könnte einfach übergeben werden. Wenn die Besitztransaktion aber anonym geschehen soll, dann kann die Übergabe nicht auf so einfachem Wege stattfinden, da sie die Identifikation der beiden Partner voraussetzt.

Eine mögliche Lösung wäre das Einschalten eines Treuhänders, aber auch bei einer solchen Transaktion muss ein Mindestmaß an Kommunikation zwischen den beiden beteiligten Partnern stattfinden. Die Transaktionsnummer muss beiden bekannt sein. Eine mögliche, aber sehr umständliche Lösung wäre der analoge Weg. Der ursprüngliche Besitzer lässt auf einem geeigneten Display die Transaktionsnummer anzeigen, die der zukünftige Besitzer mit einem Gerät einliest. Dies ist sehr umständlich und nur möglich, wenn es sich um lokale Transaktionen handelt.

Eine andere Alternative wäre die Schaffung von abgeschirmten Räumen, die eine Löschung der bisherigen Identität ermöglichen, ohne dass Dritte sich in die Besitzergreifung einmischen könnten. Aber auch diese Lösung ist nur mit einigem Aufwand verbunden. Eine sichere und einfache Lösung dieses Problems muss noch gefunden werden.

8.3 VERTRAUEN IN DIE KOMMUNIKATIONSPARTNER

Zwar kann mit dem Privatsphärenmodell klar reglementiert werden, wer welche Daten erhält, aber es kann nicht davor schützen, dass einmal zur Verfügung gestellte Daten anders als gedacht genutzt werden. Es wäre zwar auch möglich, alle personenbezogenen Daten, egal wo sie entstehen, nur verschlüsselt zu kommunizieren und zu speichern und dann dem Kommunikationspartner bei Bedarf die Zugangsrechte zu verwehren, aber ein solches System könnte immer auch umgangen werden, wenn der Wille bestünde. Zudem würde es einen enormen Verwaltungsaufwand zusätzlich bedeuten. Kurz, wenn man mit jemandem kommuniziert, muss das auf einer Vertrauensbasis geschehen. Das Privatsphärenmodell ist nicht geeignet, als DRM-System genutzt zu werden. Wenn ich jemandem nicht vertraue, dann sollte ich ihm keine Daten geben.

9.1 BEISPIEL »CHARLOTTE COMMUNICATIVE«

Charlotte hat gerne mit Menschen zu tun und teilt sich auch gerne mit. Deswegen landen alle Identitäten und Dienste per Voreinstellung im privaten Bereich. Denn auch wenn Charlotte gerne kommuniziert, so musste sie doch feststellen, dass zu große Offenheit manchmal sehr lästig ist. Daher hat sie für ihre Freunde spezielle Kommunikationsidentitäten angelegt. Ebenso möchte sie sich nur von ihren Freunden aufspüren lassen und hat deswegen alle Lokalisierungsdienste in der privaten Ebene. Eine Ausnahme macht sie für den neuen Dating-Service »Find Your Love«, da sie momentan Single ist und sie das gerne ändern würde. Es ist jedes Mal spannend, wenn das kleine Plastikherz piept, auch wenn der Traummann noch nicht dabei war. Viele scheinen ihre Profile beim Datingservice ein wenig zu optimistisch zu gestalten.

Charlotte macht gerne auch ihre Freundinnen ein wenig neidisch, wenn es um die neuesten Modetrends geht. Deswegen hat sie auch die Identifikationsdienste alle in der privaten Ebene. So können wissen ihre Freundinnen immer sofort bescheid, dass sie etwas neues hat, und das nächste Gesprächsthema ist schon sicher.

Ganz selten will aber auch Charlotte einmal ihre Ruhe. Dann aber auch ganz und gar. Auch vor ihren eigenen Technologien. Deswegen sind in ihrem persönlichen Bereich keine Identitäten zu finden. Will sie für sich bleiben stellt sie ihre Kommunikationseinstellung auf persönlich und hat vollständig Ruhe.

GENERAL RULE: All Identities and related services are private

FRIENDS

Alexander Stephen Marten Noah John Christine
Susan Anna Carl Sophie Francis Hank Michal
Julia Simone Philipp Paolo Luke George Stan Oliver

IDENTIFICATION SERVICES

PUBLICATON SERVICES

COMMUNICATION SERVICES

forfriends@charlotte.net

IM-Identity for friends

telephone

public@charlotte.net

IM-Identity for public

LOCALISATION SERVICES

Mobile Findr™

Where Are You?™

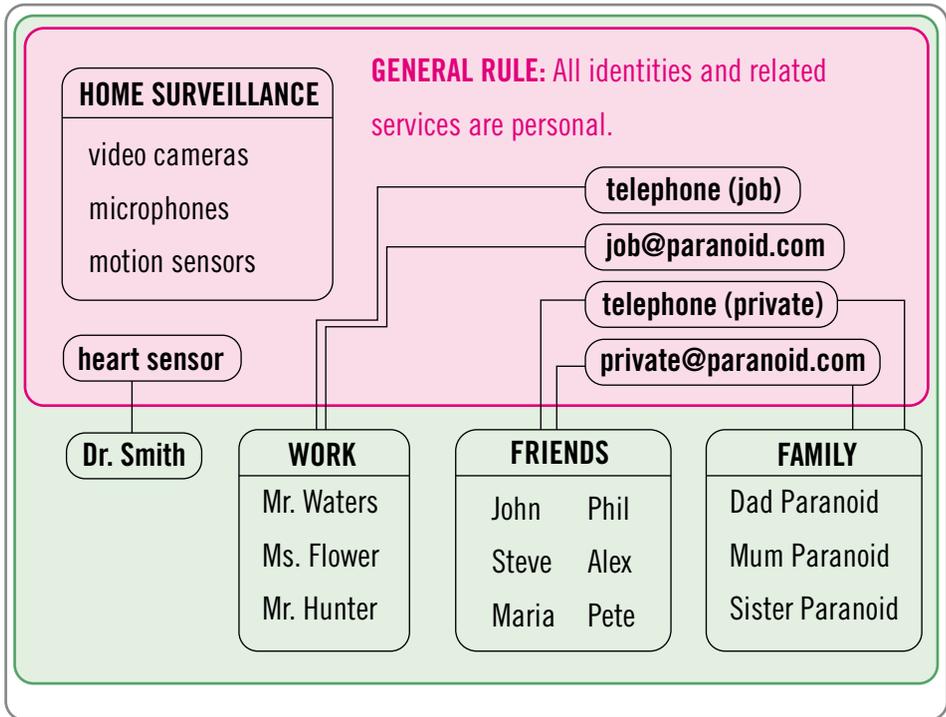
Find Your Love!™

9.2 BEISPIEL »PETE PARANOID«

Pete hat gerne seine Ruhe. Deswegen ist beim ihm per Voreinstellung nicht nur die öffentliche Sphäre deaktiviert, sondern alle Dienste landen immer in der persönlichen Sphäre. Er wählt sorgfältig aus, wer mit ihm kommunizieren darf. Da er ohnehin wenig Lust auf Kommunikation hat, beschränkt sich dabei der Einstellungsaufwand enorm. Nur sehr selten muss er neue Fremdidentitäten hinzufügen. Die meisten Personen oder Institutionen will er garnicht kennen.

Leider hat Pete aber Herzrhythmusstörungen und ist auch sonst nicht bei bester Gesundheit. Der Sensor, der notwendigerweise sein Herz überwacht, funkt deswegen auch immer zu seinem Arzt, damit dieser bei kritischen Situationen sofort informiert ist. Aber selbst diese vielleicht lebenswichtige Kommunikation, will Pete manchmal nicht haben. Deswegen liegen Arzt und Sener getrennt voneinander. Sein Arzt hat in zwar davor gewarnt, dass eine solche Einstellung in der falschen Situation fatal sein könnte, aber Pete kann sich einfach nicht dazu durchringen auch nur von einer Person permanent überwachbar zu sein.

Um auch wirklich seine Ruhe zu haben, hat Pete zusätzliche Regeln für die Kommunikation aufgestellt. Seine Arbeitskollegen können ihn nur von 8 bis 19 Uhr erreichen. Anrufe und Nachrichten, die in dieser Zeit eingehen, werden ihm beim Frühstück zugestellt. Pete liebt diese Kontrolle über seine Privatsphäre, und deswegen liebt er besonders seine Überwachungsanlage Zuhause. Egal wo er ist, er kann ständig überprüfen ob bei ihm eingebrochen wurde. Er wurde zwar schon zweimal von einem Fehlalarm aufgeschreckt, weil der Aushilfpostbote vom Überwachungssystem fälschlicherweise als Einbrecher klassifiziert wurde, aber Pete meint: »lieber ein Fehlalarm, als keine Überwachung.



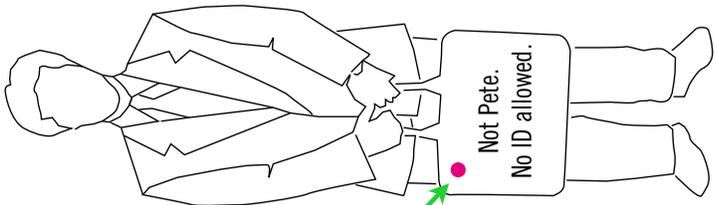
9.3 SZENARIO »STYL R FINDR«

Anna hat sich ein neues Mobiltelefon zugelegt, das eine NFC-Shell besitzt. Was letztlich nichts anderes ist als ein RFID-Lesegerät. Um dieses auch nutzen zu können, hat Anna den Dienst »Styl R Findr« gebucht, mit dem sie zu ausgelesenen RFID-Tags Informationen wie Preis, Hersteller und Verkaufsstellen angezeigt bekommt.

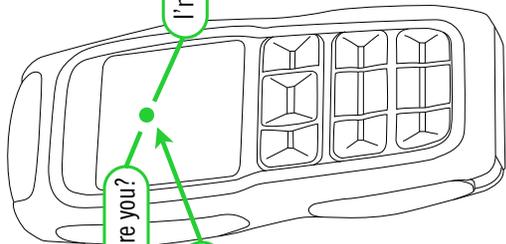
Da Anna eine Freundin von Charlotte Communicative ist, ist sie genauso wie die Identifikationsdienste von Charlottes Kleidung in Charlottes privater Ebene und deswegen wird eine Kommunikation zwischen NFC-Mobiltelefon und RFID-Tags möglich. Die RFID-Tags in Charlottes Kleidung prüfen dafür, ob sie Anna kennen, und was sie ihr mitteilen dürfen. Würde Anna gerade ihre Ruhe haben wollen, und hätte ihre Privatsphäre auf persönlich eingestellt, würde diese Kommunikation jedoch nicht stattfinden, da alle Dienste in der privaten Ebene stumm geschaltet wären.

Anders sieht dies bei Pete Paranoid aus. Er kennt Anna nicht und seine Identifikationsdienste dürfen nur ihm persönlich Auskunft erteilen. Dementsprechend bleibt der RFID-Tag von Petes Tasche stumm, als Annas Anfrage kommt. Da die Kommunikation von Anna ausgeht, muss sie sich zwar gegenüber Petes Tasche identifizieren, aber Petes Tasche bleibt anonym, da sie einfach nicht antwortet. Was Anna sehr bedauerlich findet, da diese Tasche das perfekte Geschenk für ihren Vater wäre. Sie traut sich jedoch auch nicht Pete direkt anzusprechen, weil er so griesgrämig dreinschaut.

Pete



Anna's
NFC mobile phone

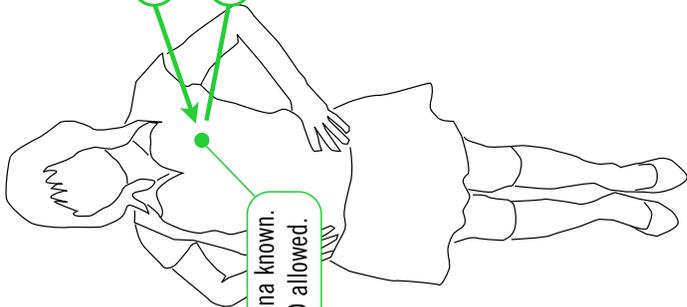


I'm Anna's NFC. Who are you?

I'm Anna's NFC. Who are you?

I'm a Shirt by Guppi.

Charlotte



Anna known.
ID allowed.

Nachwort

Nachdem nun die Probleme und aktuellen Tendenzen der Nutzung von ICT und UCT aufgezeigt wurden und nachdem nun ein Vorschlag im Raum steht, wie man anders mit den Technologien umgehen könnte, um die Wahlfreiheit beim Schutz der Privatsphäre zu gewährleisten, stellt sich die Frage, wie es weitergeht. Könnte ein solches System tatsächlich irgendwann zur Verfügung stehen?

Ein Vorteil dieses Privatsphärenmodells ist, dass es beispielsweise bei den Identitäten bereits existierende Bemühungen aufgreift. Die Notwendigkeit, eine einfache Verwaltung von digitalen Identitäten zu ermöglichen, ist längst bekannt und es wird an Lösungen gearbeitet. Für das Privatsphärenmodell müssten solche Systeme im Prinzip nur erweitert werden.

Auch die Notwendigkeit, Kommunikation ausschließlich verschlüsselt zu betreiben, ist längst erkannt und wird in vielen Bereichen bereits praktiziert. In der Summe stehen die Technologien und Teilanwendungen, die als Ganzes zum Privatsphärenmodell führen würden, bereits heute zur Verfügung oder zumindest in absehbarer Zeit.

Auch die Verwaltung der Privatsphäre ist an heutige Interfaces angelehnt und bedient sich so bereits erlernter Methoden. Dabei integriert sich die Verwaltung der Privatsphäre so sehr, dass sie in der normalen Verwaltung der Kommunikation fast verschwindet. Nur in bewussten Sonderfällen tritt sie wieder zutage und verlangt eine Nutzerinteraktion. Auch von diesem Standpunkt aus gibt es wenig, was einer Implementation des Privatsphärenmodells im Wege steht. Ganz im Gegenteil würden es sicher viele Nutzer begrüßen, wenn sie ihre Kommunikation endlich zentral verwalten könnten und nicht ständig an verschiedenen Stellen nachbessern müssten.

Kurzum, in Einzelteilen werden alle Elemente des Privatsphärenmodells bereits verfügbar oder werden es bald sein. Die grundlegende Forderung nach Transparenz und Offenheit der Systeme wird dabei jedoch auf der Strecke bleiben. Zu groß dürfte das Interesse der Unternehmen sein, nicht nur mit Dienstleistungen um die Privatsphäre Geld zu verdienen, sondern auch mit dem Produkt Privatsphäre.

Das größte Problem in der Realisierung eines Gesamtsystems ist dabei sicherlich auch der Umstand, dass zwischen Technologiewelten, die heute noch nichts miteinander zu tun haben, neue Brücken geschlagen werden müssen. Interoperable Protokolle beziehungsweise standardisierte Schnittstellen, die in die Mittlerrolle treten, werden auf allen Ebenen notwendig sein und existieren heute teilweise noch nicht. Vielfach, weil sich Unternehmen nicht einigen können, wie am Beispiel Wireless USB aktuell. Als Kompromiss gedacht, sind beide beteiligten Parteien damit unglücklich und wollen jeweils ihre eigenen Standards weiterentwickeln. Auch Probleme wie Lizenzgebühren und die umstrittenen Softwarepatente werden ein offenes und herstellerunabhängiges System zum Schutz der Privatsphäre auf absehbare Zeit nicht entstehen lassen.

Zudem fehlt der politische Wille dazu, würde doch ein solches System auch viele Überwachungsmöglichkeiten zunichte machen. Doch gerade die werden momentan immer häufiger genutzt oder implementiert. Die Lobby der Datenschützer und Privatsphärenverfechter ist heute machtlos gegenüber den Begehrlichkeiten der Regierungen. Für die Informationsgesellschaft, die so gerne als bessere Zukunft dargestellt wird, eigentlich eine Unmöglichkeit. Die Diskussion um eine vierte Macht im Staat muss dringend erfolgen. Dass die Privatsphäre schützbar wäre, zeigt diese Arbeit.

Auf der anderen Seite ist das aufgezeigte Privatsphärenmodell aber auch nur ein Kompromiss. Es akzeptiert, dass es andere Grenzen für die Privatsphäre gibt, wenn wir Technologie einsetzen und nutzen wollen. Diese Zugeständnisse gehen an einigen Stellen sicherlich weiter, als sie viele Datenschützer und Privatsphärenlobbyisten heute ziehen einräumen. Aber wie bereits im Vorwort zu dieser Arbeit geschrieben, stellt diese Arbeit ein Konzept für eine Privatsphäre in einer Ubiquitous Computing-Zukunft dar. Sie ist nicht dafür gedacht, die gegenwärtigen Vorstellungen von der Limitierung der Technologie an sich umzusetzen. Angesichts der gegenwärtigen Entwicklung scheint ein generelles Ablehnen der Technologie als Lösung für den Schutz der Privatsphäre nicht sinnvoll.

Dennoch haben die Datenschützer recht in ihren Bestrebungen. Solange solche Lösungen, wie das hier vorliegende Privatsphärenmodell, nicht implementiert sind, kann jede weitere Technologie nur dazu geeignet sein, unsere Privatsphäre weiter einzuschränken.

Das fatale an der heutigen Situation ist eben das »Privacy as default«. Ohne Interesse für das Thema wird kaum jemand bemerken, dass seine Privatsphäre verletzt wird, bis es zum Auftreten spürbarer negativer Folgen kommt. Deswegen bleibt nur die kritische Gegnerschaft gegenüber den Technologien und ihren Anwendungen, bis diese unter der Prämisse »Privacy by default« stehen, auch wenn die Privatsphäre sich in der Informationsgesellschaft anders definieren wird, als sie es heute tut.

Anhang

0–9 3GPP 3rd Generation Partnership Project
Zusammenschluss verschiedener Standardisierungsgremien, um weltweite Interoperabilität der 3rd-Generation-Mobilnetze sicherzustellen.
<<http://www.3gpp.org>>

802.11

IEEE Standardset für alles WLAN-betreffende. s.a. Wi-Fi
<<http://grouper.ieee.org/groups/802/11>>
<http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm>

802.15

IEEE Standardset für alles WPAN-betreffende. s.a. Bluetooth, ZigBee
<<http://grouper.ieee.org/groups/802/15>>

802.16

IEEE Standardset für alles WMAN-betreffende. s.a. WiMAX
<<http://grouper.ieee.org/groups/802/16>>

A ad-hoc-Netzwerk

Verbindung von Endgeräten per Funknetz ohne zusätzliche Infrastruktur. Das Aushandeln der Verbindung übernehmen die Geräte selber. Beispielsweise die Bluetoothverbindung zwischen Headset und Mobiltelefon oder die Verbindung zweier WLAN-fähiger Endgeräte ohne Accesspoint.

AES Advanced Encryption Standard

Verschlüsselungsalgorithmus, der bei WPA2 zum Einsatz kommt.
Standard: IEEE 802.11i

AIDC Automatic Identification and Data Capture
Technologien vor allem zur Kontrolle von Warenbewegungen. Barcode, RFID, EPC.

AJAX Asynchronous Javascript and XML
Umschreibung für die neueste Form der Realisierung interaktiver Web-Applikationen. Durch die clientseitige Ausführung der meisten Operationen (Javascript) und dem partiellen Nachladen einzelner Daten und nicht einer ganzen Seite ist ein flüssigeres Arbeiten möglich als mit herkömmlichen Serverseitigen Applikationen. AJAX ist dabei weder eine neue Technologie noch ein Standard, sondern eher ein neues Buzzword.

<<http://www.adaptivepath.com/publications/essays/archives/000385.php>>
<<http://en.wikipedia.org/wiki/AJAX>>

AMI Ambient Intelligence

Die intelligente kommunizierende Umgebung. Synonym mit Ubicomp. s.a. Internet of Things.

Asterisk

Open-Source-VoIP-Lösung. Als vollständige Alternative zu anderen VoIP-Systemen existieren sowohl Asterisk-Serversoftware, Soft-Phones und auch Gateways ins Festnetz. Das verwendete Protokoll IAX2 ist ebenfalls Open Source, so ist eine hohe Transparenz sichergestellt, im Gegensatz zu etwa Skype mit ihrem proprietären Closed-Source-Ansatz.
<<http://www.asterisk.org>>
<<http://www.asteriskguru.com>>

Asymmetric Key**Asymmetrische Verschlüsselung**

s. Public Key

B Backbone

Grundlegende Internet-Infrastruktur. Verbindet Kontinente und Regionen über Hochleistungsglasfasernetze. s.a. IP-Carrier und WAN.

BfDI Der Bundesbeauftragte für Datenschutz und Informationsfreiheit

<<http://www.bfdi.bund.de>>

Bluetooth

Standard IEEE 802.15.1 zur (ad-hoc) Vernetzung einzelner Geräte (Mobiltelefone, Computer oder Peripherie). Reichweite beträgt nur wenige Meter. Fällt unter den Oberbegriff WPAN.

<<https://www.bluetooth.org>>

<<http://www.ieee802.org/15/pub/TG1.html>>

<<http://www.palowireless.com/bluetooth>>

<<http://en.wikipedia.org/wiki/Bluetooth>>

Broadband

Oberbegriff für drahtgebundene Internetanschlüsse mit hoher Datenübertragungsrate. Schließt Übertragung über Glasfaser, TV-Kabel und Kupferkabel (DSL) ein.

Bruteforce

Sprichwörtlich „die rohe Gewalt“, mit der versucht wird, durch reines Ausprobieren möglicher Schlüssel auf verschlüsselte Daten zuzugreifen. Als sicher gelten momentan Schlüssel mit 4096bit Länge, da diese so viele Möglichkeiten bieten, dass selbst Supercomputer sie nicht in angemessener Zeit durchprobieren können. Die elegante andere Methode, um Verschlüsselungen zu knacken, ist das Finden von Fehlern im Algorithmus der Schlüsselerzeugung oder deren Implementation.

C Cable Spaghetti

Der Zustand, den heutige Computer und Elektrogeräte durch die hohe Anzahl von Kabeln erzeugen. Einer der Gründe, verstärkt auf drahtlose Kommunikation zu setzen.

<http://en.wikipedia.org/wiki/Cable_spaghetti>

Car2Car Car to Car

Funkkommunikation zwischen Autos in einem ad-hoc-Verfahren. s.a. P2P

Standard: IEEE 802.11p (WAVE)

<<http://www.car-to-car.org>>
<<http://www.heise.de/tr/artikel/72500>>

CCC Chaos Computer Club e.V.

Aktivisten für Datensicherheit und -schutz.
<<http://www.ccc.de>>

CCL Congestion Charging London

Bezahl- und Regulationssystem für die Auto-nutzung in Londons Innenstadt.

<http://www.tfl.gov.uk/tfl/cclondon/cc_intro.shtml>

Closed Source

Software, die nur als fertige Anwendung veröffentlicht wird. Der Quellcode bleibt geheim. Gegenteil von Open Source.

CORDIS Community Research & Development Information Service

CORDIS is an information space devoted to European research and development (R&D) and innovation activities.

<<http://cordis.europa.eu/en/home.html>>

D Data Mining

Sammlung, Aufbereitung und Speicherung von persönlichen Daten, um möglichst detaillierte Profile zu erstellen. Datenschutzrechtlich fragwürdig bis illegal.

DRM Digital Rights Management

Systeme zur Kontrolle des Zugangs zu (Medien-)Daten. Schutz vor unerlaubter Nutzung, etwa dem Kopieren von Daten. Von Kritikern auch Digital Restrictions Management genannt.

DSL Digital Subscriber Line

Breitbandiger Internetzugang über Kupfertelefonkabel.

DVB Digital Video Broadcasting

Digitalrundfunk für Fernsehen und Radio. Kommt in verschiedenen Formaten. DVB-S für Satellitenübertragung, DVB-T für terrestrischen Rundfunk, DVB-C für TV-Kabelübertragung und als Besonderheit für mobiles Fernsehen DVB-H für Handhelds.

<http://de.wikipedia.org/wiki/Digital_Video_Broadcasting>
<<http://www.ueberallfernsehen.de>>

E EAN European Article Number

Die Nummer, die auf jedem Produkt als Barcode abgebildet ist. Mittlerweile weltweit in Verwendung.

<http://en.wikipedia.org/wiki/European_Article_Number>
<<http://www.gs1.org/productssolutions/barcodes>>

EDGE Enhanced Data Rates for GSM Evolution

Beschreibt eine Technik, um die Datenübertragungsraten in GSM-Netzen zu erhöhen. Die erreichbare maximale Übertragung beträgt 384kb.

<<http://de.wikipedia.org/wiki/EDGE>>

EDV Elektronische Datenverarbeitung

Formaldeutscher Begriff für alles, was mit computergestützter Datenverarbeitung zu tun hat. Veraltet, da dies heute auf fast alle Informationsverarbeitungen zutrifft.

EFF Electronic Frontier Foundation

Amerikanische NGO zum Schutz der digitalen Bürgerrechte.

<<http://www.eff.org>>

EITO European Information Technology Observatory
Jährliche Veröffentlichung einer Analyse der europäischen ICT-Landschaft.
<<http://www.eito.org/index-eito.html>>

ePaper Electronic Paper
Elektronisches Papier. Mehrere Hersteller arbeiten an solchen Technologien, die dynamische Displays mit den Qualitäten von Papier ermöglichen sollen. Sehr ähnlich oder identisch zu eInk-Konzepten. Die ersten marktreifen Anwendungen werden Ende 2006 erscheinen.
<<http://www.eink.com>>
<<http://www.irextechnologies.com/home.htm>>
<<http://en.wikipedia.org/wiki/EPaper>>
<http://en.wikipedia.org/wiki/Electronic_ink>

EPC Electronic Product Code
<<http://www.epcglobal.de>>
<http://de.wikipedia.org/wiki/Elektronischer_Produktcode>

ETSI
European Telecommunications Standards Institute
Standardisierungsgremium der europäischen Mobilfunkanbieter. Hat Standards wie GSM und HIPERMAN festgelegt. s.a. 3GPP.
<<http://www.etsi.org>>

F **FIP** Fair Information Practice
Richtlinien für den fairen Umgang mit personenbezogenen Daten hinsichtlich des Datenschutzes und des Schutzes der Privatsphäre. s. Literaturliste: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

FOMA Freedom of Mobile Multimedia Access
Japanischer 3G Telekommunikationsstandard. Kompatibel mit UMTS.
<http://en.wikipedia.org/wiki/Freedom_of_Mobile_Multimedia_Access>

G **GPRS** General Packet Radio Service
Erweiterung des GSM-Standards um paketorientierte Datenübertragung.
<<http://de.wikipedia.org/wiki/GPRS>>

GPG GNU Privacy Guard
Open Source Variante von PGP. Unterstützt den OpenPGP-Standard.
<<http://en.wikipedia.org/wiki/GPG>>
<<http://en.wikipedia.org/wiki/OpenPGP>>

GPL General Public License
Eine Lizenz, unter der Open-Source-Quellcode (OSS) veröffentlicht werden kann. Wer GPL-lizenzierten Code verwendet, muss die derivative Arbeit auch wieder unter der GPL veröffentlichen. Neben der GPL gibt es noch andere Lizenzen, um OSS zu veröffentlichen.
<<http://en.wikipedia.org/wiki/GPL>>

GPS Global Positioning System
Satellitennavigationssystem, betrieben von den USA. Ein Konsortium aus EU-Ländern installiert gerade das äquivalente Galileo-System.

GSM Global System for Mobile communications
Digitaler Mobilfunkstandard. In Deutschland Basis für D- und E-Netz.
<<http://www.gsmworld.com/index.shtml>>
<http://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications>

GUI Graphical User Interface

H **H2G2** The Hitchhiker's Guide to the Galaxy
Handset-Universallexikon aus dem gleichnamigen Roman von Douglas N. Adams. Eine der bekanntesten frühen Visionen für angewandtes Pervasive Computing. Besonders hervorzuheben ist die Aufschrift in freundlichen Lettern: »Don't Panic«. Für die »Earth Edition« siehe:
<<http://www.bbc.co.uk/dna/h2g2>>

Handover
Übergabe der Verbindung eines Endgeräts zwischen (benachbarten) Netzknoten infrastruktureller Netzwerke ohne Unterbrechung der Verbindung.
<<http://en.wikipedia.org/wiki/802.11r>>

Hash-Funktion
Anhand einer Hash-Funktion, die der Bildung einer Quersumme entspricht, kann überprüft werden, ob ein Datenpaket verändert wurde. Der Erzeuger des Datenpakets oder der Dateneinheit erzeugt die Hash-Checksum einmal und verbreitet sie mit der Dateneinheit. So wird überprüfbar, ob es Abweichungen vom Original gibt. Gebräuchlichstes Verfahren ist MD5, das allerdings mittlerweile als unsicher gilt; und daher SHA-1 propagiert wird.
<http://en.wikipedia.org/wiki/Cryptographic_hash_function>

HCI Human Computer Interface

HIPERACCESS

Grundlegende Standards der ETSI für Wireless Broadband Access.
<<http://portal.etsi.org/radio/HiperAccess/HiperAccess.asp>>

HIPERLAN

ETSI Konkurrenzstandardset zu 802.11.
<<http://portal.etsi.org/radio/HiperLAN/HiperLAN.asp>>

HIPERMAN

High Performance Metropolitan Area Network
Europäischer Standard für Funknetzwerke und -technologien der ETSI. Mittlerweile harmonisiert mit dem WiMax-Standard 802.16-2004.
<<http://portal.etsi.org/radio/HiperMAN/HiperMAN.asp>>

HSCSD High-Speed Circuit-Switched Data

Protokollerweiterung für GPRS-Netze, um Datenübertragung zu optimieren. Alternative zu GPRS.
<<http://en.wikipedia.org/wiki/HSCSD>>

HSDPA High Speed Downlink Packet Access

Protokoll für schnelle Datenübertragung via UMTS-Netze.
<http://en.wikipedia.org/wiki/High-Speed_Downlink_Packet_Access>

i2010

EU-Initiative zur Förderung und Erforschung der europäischen Informationsgesellschaft. s. Literaturliste

IAX Inter-Asterisk eXchange protocol

Kommunikationsprotokoll der Open-Source-VoIP-Lösung Asterisk.
<<http://en.wikipedia.org/wiki/IAX>>

ICT Information and Communication Technology

Oberbegriff für alle Technologien, die in der Informationsgesellschaft Anwendung finden.

IEEE

Institute of Electrical and Electronics Engineers
Non-Profit-Organisation für die Entwicklung von IT-Standards, insbesondere Netzwerkstandards. s.a. WLAN, WiMAX
<<http://www.ieee.org>>

IETF Internet Engineering Task Force

Non-Profit-Organisation zur Entwicklung von Internetstandards, insbesondere TCP/IP und ähnliche Kommunikationsstandards.
<<http://www.ietf.org>>
<<http://www.ietf.org/rfc/rfc3160.txt>>

IKT Informations- und Kommunikations-Technologie
s. ICT

IMS IP Multimedia Subsystems

Systeme und Protokolle, die auf IP basieren und für die Übermittlung von Film- und Tonmedien ausgelegt sind.

Internet of Things Das Internet der Dinge

Oberbegriff für den Teilbereich der UC-Technologien, die alle Objekte Informationen kommunizieren und verarbeiten lassen. s.a. Ubicom.

IP Internet Protocol

Basisprotokoll für Datennetzwerke. Die Mehrheit der heutigen IT-Netzwerke fußt auf diesem Standard. Heute werden noch fast überall Netzwerkadressen nach IPv4-Standard vergeben (111.222.333.444). Der Adressraum in IPv4 ist auf 4,3 Milliarden begrenzt, was absehbar zu wenig ist, daher wurde IPv6 eingeführt, das 340 Sextillionen (3,4x10³⁸) Adressen bietet und damit auf absehbare Zeit genug.
<http://en.wikipedia.org/wiki/Internet_Protocol>
<http://en.wikipedia.org/wiki/Internet_protocol_suite>

IP-Carrier

Betreiber von Internet-Backbonestrukturen. Beispielsweise Colt, AT&T oder T-Com.

IPsec Internet Protocol Security

Protokoll zum Authentifizieren und Verschlüsseln von IP-Datenpaketen.

IPTV Internet Protocol TeleVision

Letztlich nichts anderes als Videostreaming, jedoch in Angebotsstruktur und Zugang an das klassische Fernsehen angelehnt. Wesentliches Element von Triple Play-Angeboten.

IrDA Infrared Data Association

Nahbereichsfunknetzwerk mit niedriger Übertragungsrate. Erfordert Sichtverbindung zwischen den Kommunikationspartnern. Wird heute eingesetzt zur direkten Kommunikation zwischen Handsets, Computern und Mobiltelefonen.

<<http://www.irda.org>>

<<http://en.wikipedia.org/wiki/IrDA>>

ISA Intelligent Software Agent

Konzept, das vorsieht, dass Programme autonom Informationen filtern, kommunizieren und für den Nutzer aufbereiten.

ISM-Band Industrial, Scientific and Medical Band

Lizenz- und genehmigungsfreie Frequenzbänder für Sendegeräte. Unter anderem nutzen WLAN, Bluetooth, RFID diese Frequenzbänder. International sind unterschiedliche Frequenzbänder freigegeben.

<<http://www.itu.int/ITU-R/terrestrial/faq/index.html>>

<<http://de.wikipedia.org/wiki/ISM-Band>>

IST Information Society Technologies

Oberbegriff für alle Technologien, die in der Informationsgesellschaft Anwendung finden. s.a. ICT, WSIS, ISTAG

ISTAG IST Advisory Group

EU-Forschungsprojekt zur Entwicklung und Implementation von IST auf EU- und EU-Länderebene.

<<http://cordis.europa.eu/ist/istag.htm>>

IT Information Technology

Oberbegriff für alle Informationsverarbeitenden Technologien. Leicht veraltet, wird IT mehr und mehr durch ICT ersetzt.

ITS Intelligent Transportation Systems

Ubicomp im Straßenverkehr.

<<http://portal.etsi.org/radio/IntelligentTransportSystems/ITS.asp>>

ITU International Telecommunication Union

UN Organisation zur Koordinierung der weltweiten Telekommunikation. Vermittelt zwischen Regierungen und privatwirtschaftlichen Unternehmen. Organisiert Konferenzen wie WSIS.

<<http://www.itu.int>>

LAN Local Area Network

Lokales, also räumlich und/oder logisch begrenztes Netzwerk. Üblicherweise geschlossenen und drahtgebunden. Mehrere LANs können per WAN verbunden werden. s.a. WLAN

LCD Liquid Crystal Display

Flüssigkristallbildschirm. Wird mittelfristig wohl vollständig von OLED-Displays abgelöst. s.a. TFT

<<http://de.wikipedia.org/wiki/F1%C3%BCssigkristallbildschirm>>

<http://www.beamer.de/produkte/lcd/lcd-tft_technik-anwendung.html>

LED Light Emitting Device/Diode

Die klassischen LEDs, basierend auf anorganischen Polymerstrukturen (auch als PLEDs im Unterschied zu OLEDs bezeichnet).

<<http://de.wikipedia.org/wiki/LED>>

LBS Location Based Services

Standortabhängige Informationsdienste, wie die Abfrage nach umliegenden Geschäften.

M **MAC(-Adresse)** Media Access Control-Adresse

Tiefe Schicht im OSI-Modell für Netzwerkprotokolle. Jede übliche Netzwerkschnittstelle hat eine MAC-Adresse als eindeutig identifizierbare Nummer. MAC-Adressen werden weltweit jeweils nur einmal vergeben.

<http://en.wikipedia.org/wiki/Media_Access_Control>

<http://en.wikipedia.org/wiki/MAC_address>

MAN Metropolitan Area Network

Großräumiges Netzwerk mit bis zu 100km Größe. Heute sind damit ausschließlich drahtgebundene Infrastrukturnetzwerke gemeint, die als Backbone etwa für Firmen-LANs oder das Internet fungieren. s.a. WMAN.

<http://de.wikipedia.org/wiki/Metropolitan_Area_Network>

MANET Mobile Ad-hoc Network

Konzept für infrastrukturlose P2P-Netzwerke.

<<http://www.ietf.org/html.charters/manet-charter.html>>

Man-In-The-Middle Attack

Eine Form des Angriffs auf eine Kommunikation zwischen zwei Endpunkten. Der heutige Datenverkehr wird nicht unmittelbar zwischen den Endpunkten hin und her geschickt, sondern durchläuft viele Knoten. Man-In-The-Middle-Angriffe finden so statt, dass Zugang zu einem dieser Knoten erlangt wird und die darüber laufende Kommunikation abgehört oder verfälscht wird. Die Wahrscheinlichkeit der Entdeckung eines solchen Angriffs ist sehr gering. Ein Netz ist aufgrund solcher Angriffsmöglichkeiten immer nur so sicher wie das schwächste Glied.

MBWA Mobile Broadband Wireless Access

Standard für mobile und high-speed mobile Funknetze. In gewissen Bereichen in direkter Konkurrenz zu WiMAX. Standardset: 802.20 <<http://grouper.ieee.org/groups/802/20/index.html>>

MEAT™ MeshNetworks Enabled Architecture™

Wi-Fi-Komplettsystem von Motorola, um Städte mit Meshed Networks und darauf basierenden Diensten zu versehen. <http://www.motorola.com/governmententerprise/northamerica/en-us/public/functions/browsesolution/browsesolution.aspx?navigationpath=id_804i/id_2523i>

Meshed

Netzwerktopologie für Funknetzwerke, in der alle sich überlappenden Knotenpunkte miteinander kommunizieren. Hohe Ausfallsicherheit, da Daten über beliebige Strecken geroutet werden können. Für WLANs nach 802.11 wird am Standard s gearbeitet.

<http://www.moskaluk.com/Mesh/wireless_mesh_topology.htm>

<http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm>

MIFARE™

Markenname für kontaktlosen Smartcard-Standard von Philips Semiconductors Standard: ISO 14443A <<http://www.mifare.net>>

Mobile-Fi Mobile Fidelity

s. MBWA

MPS™ MeshedNetworks Positioning System

Teil des Motorola MEA Konzepts. s.a. WPS.

MRZ Machine Readable Zone

Bereiche auf Objekten, die visuell von Scannern ausgelesen und als Daten interpretiert und verarbeitet werden können. Das bekannteste Beispiel ist der Barcode.

Mu-Fi Municipal Wi-Fi

Privat organisierte WLANs.

<<http://freifunk.net>>

<<http://www.seattlewireless.net>>

N NFC Near Field Communication

Oberbegriff für Funkstandards und -technologien, die nur auf wenige Meter oder Zentimeter Entfernung funktionieren. Auch Name eines Industriekonsortiums (Nokia, Siemens, etc.), das Technologien auf Basis von RFID vorantreibt.

<<http://www.nokia.com/nfc>>

<<http://www.nfc-forum.org>>

O OECD Organisation for Economic Co-operation and Development

Transnationale Organisation zur Förderung des weltweiten Handels, sozialer Marktwirtschaft und Demokratie. Mitgliedsländer sind u.a. Deutschland, Frankreich, Japan, UK, USA. Erstellt umfangreiche Analysen zu den verschiedenen Aspekten der Gesellschaft und der Wirtschaft.

<<http://www.oecd.org>>

<<http://www.sourceoecd.org>>

OLED Organic Light Emitting Device/Diode

Displaytechnologie, auf organischen Substanzen basierend. Viele Vorteile gegenüber klassischen LEDs.

<<http://de.wikipedia.org/wiki/OLED>>

<<http://www.universaldisplay.com/tech.htm>>

OLSR Optimized Link-State Routing

Routing-Protocol für Mesh-WLANs. Im Einsatz u.a. im Berliner Freifunk-Netz.

<<http://www.ietf.org/rfc/rfc3626.txt>>

OMA Open Mobile Alliance

Industriekonsortium zur Sicherstellung der Interoperabilität und Förderung von Mobil-Technologien.

<<http://www.openmobilealliance.org>>

OpenPGP

s. PGP

Open Source

Prinzip, nach dem Software samt Quellcode veröffentlicht wird und offen zugänglich ist. Der Quellcode wird dabei unter Lizenzen wie der GPL veröffentlicht. Gegenteil von Closed Source.

ÖPNV Öffentlicher PersonenNahVerkehr**OS** Operating System

Betriebssystem eines Computers oder ähnlichen Geräts.

OSI Model Open Systems Interconnection Reference Model

Abstraktes Modell zur Beschreibung der Struktur eines Kommunikationsnetzwerks. Besteht aus sieben Ebenen. Viele moderne Standards für Netzwerke basieren auf diesem Modell.

<http://en.wikipedia.org/wiki/OSI_model>

OSS Open Source Software

s. Open Source

Overhead

Auch Protokoll-Overhead. Bezeichnet die Daten, die für die Kommunikation im Netzwerk verschickt werden müssen, um die eigentlichen Nutzdaten senden zu können. Idealerweise ist der Overhead so gering wie möglich, da er Übertragungskapazitäten einnimmt, die nicht mehr für Nutzdaten zur Verfügung stehen.

Oyster Travelcard

Die Oyster Travelcard ist eine kontaklose Smartcard, um die Zahlungs- und Autorisierungsvorgänge im Londoner ÖPNV zu beschleunigen.

<<http://www.tfl.gov.uk/tfl/fares-tickets/2006/oyster/general.asp>>

P **P2P** Peer to Peer / Point to Point

Serverloses dezentralisiertes Netzwerk. Peers/Clients verbinden sich direkt miteinander und werden so gleichzeitig zu Routern für weitere Peers. Keine Infrastruktur jenseits der logischen Verbindung der Clients notwendig.

PAN Personal Area Network

Kleinstes logisches Netzwerk. Auf eine Person und unmittelbare Umgebung beschränkt. s.a. WPAN, NFC

Percom(p) Pervasive Computing

Synonym für Ubicomp/UC.

PGP Pretty Good Privacy

Public-Key-Verschlüsselungsverfahren für E-Mails, das Mitte der 1990er von Phil Zimmerman entwickelt wurde. Ermöglicht die Authentifizierung und Verschlüsselung von E-Mails. Mittlerweile existiert auch eine Open-Source-Variante, die sich GPG nennt. PGP war die Vorlage für den OpenPGP Standard, der mittlerweile von einer Reihe von Anwendungen unterstützt wird, die damit interoperabel sind.

<<http://en.wikipedia.org/wiki/PGP>>

<<http://en.wikipedia.org/wiki/OpenPGP>>

POC Push-to-talk Over Cellular

Push-kommunikation via Mobiltelefon. Funktioniert wie Walkie-Talkie.

<http://www.openmobilealliance.org/tech/wg_committees/poc.html>

Proof-Of-Concept

Praktische Umsetzung eines Konzepts, als Beweis für seine Richtigkeit. Hauptsächlich angewandt für die Überprüfung von Sicherheitskonzepten in den ICT. Dabei geht es nicht um Anwendbarkeit im Produktionsbetrieb oder Alltagsleben, sondern darum, die grundsätzliche Möglichkeit zu beweisen. Ein Proof-Of-Concept-Virus etwa beweist die Ausnutzbarkeit einer Programmfunktion, wird aber nicht mit einer Schadfunktion ausgestattet und in Umlauf gebracht.

PTT Push-to-Talk

Synonym für POC.

Public Key

Teil eines asymmetrischen Verschlüsselungsverfahrens. Es wird ein Public und ein Private Key erzeugt. Der öffentliche ist frei zugänglich. Will jemand an den Erzeuger von der beiden Schlüssel eine Nachricht senden, wird diese mit dem öffentlichen Schlüssel verschlüsselt. Sie wird dann versendet und kann nur mit dem Secret Key,

der nur dem Erzeuger des Schlüsselpärchens zur Verfügung steht, entschlüsselt werden. Ist wesentlicher Bestandteil des OpenPGP-Verschlüsselungsverfahrens. Ebenso kann mit einem Public Key festgestellt werden, ob eine Nachricht mit dem dazugehörigen Private Key verschlüsselt wurde, bietet also eine Authentifizierungsmöglichkeit. Dennoch können aus dem Public Key keine Informationen über den Private Key gewonnen werden.
s.a. Symmetric Key
<http://en.wikipedia.org/wiki/Public-key_cryptography>

QoS Quality of Service
Sicherstellung der (möglichst) verlustfreien Übertragung von Daten in Netzwerken und der Erreichbarkeit der Netzknoten. Eine der größten Herausforderungen für Netzwerke und deren Betreiber.
<http://en.wikipedia.org/wiki/Quality_of_Service>

Quellcode
Der in einer menschenlesbaren Form verfasste Code, der nach einem Kompilierungsprozess ein fertiges Programm erzeugt. Sozusagen der Bauplan einer Software.

RFC Request For Comments
Vorveröffentlichung von Spezifikationen von Standards werden üblicherweise RFC betitelt, um sie als Diskussionsgrundlage zu kennzeichnen.

RFID Radio Frequency Identification
s.a. NFC
<http://de.wikipedia.org/wiki/Radio_Frequency_Identification>

Roaming
1. Nutzung der Netzwerke anderer Betreiber, als das, mit dessen Betreiber der Nutzer einen Vertrag geschlossen hat. Heute vorrangig für Mobilfunknetze. Voraussetzung sind Roaming-Verträge zwischen den Netzbetreibern. s.a. Handover
<<http://www.gsmworld.com/roaming/index.shtml>>
<http://www.bundesnetzagentur.de/enid/fca033c3386b1c64c20e71aed9437857,0/Regulierung_Telekommunikation/International_Roaming_2pc.html>

RTP Real-Time Transport Protocol
Protokoll zur kontinuierlichen Übertragung von AV-Daten über IP-Netzwerke. Wird u.a. von SIP zur Datenübertragung genutzt.
Standard: RFC3550
<<http://www.ietf.org/rfc/rfc3550.txt>>
<http://de.wikipedia.org/wiki/Real-Time_Transport_Protocol>

S Security by Obscurity
Die Sicherheit durch Verschleierung meint das Konzept in IT-Systemen, durch Verschleierung oder Nichtzugänglichmachung von Informationen eine Anwendung sicher zu machen. Wenn eine Anwendung nicht analysiert werden kann, weil sie verschleiert ist, soll das die Sicherheit erhöhen. Die Gefahr, dass es unbemerkelt gelingt, die Verschleierung zu umgehen und Lücken zu finden, ist jedoch gegeben. Vielfach wird daher eine Offenlegung von Programmcodes und Verschlüsselungsmechanismen gefordert, um sie offiziell und effizienter auf Schwachstellen untersuchen zu können. Die Lager Pro und Contra »Security by Obscurity« sind fast deckungsgleich mit den Open Source und Closed Source Fraktionen.
<http://en.wikipedia.org/wiki/Security_by_obscurity>

SEEMesh Simple Efficient Extensible Mesh
Protokoll für Meshed WLANs. Erarbeitet von Cisco und Intel. Wird neben Wi-Mesh die Basis für den kommenden Mesh-WLAN-Standard 802.11s bilden.

SIP Session Initiation Protocol
Offener Kommunikationsstandard für VoIP.
Standard: RFC 3261
<<http://www.ietf.org/rfc/rfc3261.txt>>
<http://de.wikipedia.org/wiki/Session_Initiation_Protocol>

Skype
Proprietäre VoIP-Technologie. Erste Geräte, die via WLAN auch mobil Skype nutzen können, kommen dieses Jahr.
<<http://www.skype.com>>

Smart Tags
Funketiketten, auf RFID basierend. Ersetzen die Barcode-Etiketten.

SRD Short Range Devices

Oberbegriff für Geräte, die über kurze Distanz funken bzw. kabellose Verbindungen aufbauen. Gemein ist diesen Geräten die Nutzung der ISM-Bänder s.a. NFC.

<http://www.bundesnetzagentur.de/enid/Allgemeinzuteilungen/Short-Range-Devices_dt.html>

<http://de.wikipedia.org/wiki/Short_Range_Devices>

<http://de.wikipedia.org/wiki/Short_Range_Devices>

SSL Secure Socket Layer

s. TSL

Symmetrische Verschlüsselung

Verschlüsselungsverfahren, bei dem ein Schlüssel Sender wie Empfänger bekannt ist. Der Sender nutzt den Schlüssel, um die Daten zu verschlüsseln. Der Empfänger nutzt den gleichen Schlüssel, um die Daten wieder zugänglich zu machen. Sicheres Verfahren, setzt aber voraus, dass der Schlüssel Sender wie Empfänger bekannt ist, aber sonst niemandem.

Wenn eine sichere Kommunikation des Schlüssels gewährleistet ist, kann mit dem One-Time-Pad-Verfahren extrem hohe Sicherheit erreicht werden. One-Time-Pads sind Schlüssel, die nur ein einziges Mal Verwendung finden.

SyncML Synchronisation Markup Language

Plattformübergreifender Standard für Synchronisation und Kommunikation mobiler Endgeräte. Festgelegt von der OMA.

<<http://www.openmobilealliance.org/tech/affiliates/syncml/syncmlindex.html>>

TCG Trusted Computing Group

Industriekonsortium, das die Spezifikationen für das TPM festlegt.

<<https://www.trustedcomputinggroup.org/home>>

<http://en.wikipedia.org/wiki/Trusted_Computing_Group>

<http://en.wikipedia.org/wiki/Trusted_Computing_Group>

TD-SCMA Time Division-Synchronous Code Division Multiple Access

3G Telekommunikationsstandard. Vorangetrieben vor allem von China, um eine mit UMTS vergleichbare Technologie zu haben, ohne Lizenzgebühren zahlen zu müssen. In das 3GPP-Standardset aufgenommen.

<<http://www.tdscdma-forum.org/EN/index.asp>>

<<http://en.wikipedia.org/wiki/TD-SCDMA>>

Telco Telecommunication**TfL** Transport for London

Das Unternehmen, das den ÖPNV in London betreibt. s.a. Oyster Travelcard

<<http://www.tfl.gov.uk>>

TFT Thin-Film Transistor

Dünnschichttransistor, der die Ausrichtung der Flüssigkristalle in LCDs steuert.

TPM Trusted Platform Module

Ein Chip, der in Geräte eingebaut wird und auf Hardwareebene Verschlüsselung, Integritätsprüfung und Digital Rights Management anbietet. Stark umstritten, da sein Design nicht offengelegt ist und somit für den Besitzer oder Nutzer eines Geräts eine Blackbox darstellt, die außerhalb der Kontrolle des Nutzers liegt. s. auch TCG.

Triple Play

Modewort für die Vereinigung von Daten-, Sprach- und Medienkommunikation über ein gemeinsames Netzwerk, etwa TV-Kabel oder DSL.

TSL Transport Socket Layer

TLS ist ein Standard zur verschlüsselten Datenübertragung im Internet. Direkter Nachfolger von SSL 3.0, ohne wesentliche Änderungen als TLS 1.0 standardisiert.

<http://en.wikipedia.org/wiki/Transport_Layer_Security>

<http://en.wikipedia.org/wiki/Transport_Layer_Security>

TUI Tangible User Interface

Ertastbare/physische Benutzerschnittstelle.

U

Ubicom(p) Ubiquitous Computing

Die Allgegenwärtigkeit von ICT, als unsichtbare Schicht der Realität. Bezieht alles, auch bisher »stumme« Objekte mit ein. Synonym mit Pervasive Computing. Mit Schwerpunkt auf Aml auch Internet of Things genannt.

UC Ubiquitous Computing

UCT Ubiquitous Computing Technologies.

s. Ubicomp

UMA Unlicensed Mobile Access

Fähigkeit von Mobile Handsets, sich je nach Verfügbarkeit mit WLAN, GPRS oder GSM zu verbinden. Unterbrechungsfreier Wechsel (Roaming) der Netzwerke auch während der Nutzung.

Beispiel: Nokia 6136 phone <<http://europe.nokia.com/nokia/0,,85001,00.html>>
<<http://netzikon.net/lexikon/u/unlicensed-mobile-access.html>>

UMTS

Universal Mobile Telecommunications System
Mobilfunkstandard der dritten Generation (3G), der GSM/GPRS ablösen soll.

<<http://www.3gpp.org>>
<http://de.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System>

UN United Nations

Die Vereinten Nationen. Dachorganisation für die ITU und damit für das WSIS.

<<http://www.un.org>>

USB Universal Serial Bus

Standard für drahtgebundene Verbindung zwischen Computer und Peripherie. 1.1 überträgt bis zu 11Mbit und 2.0 bis zu 480Mbit.

UWB Ultra Wideband

Oberbegriff für Übertragungstechnologien mit hoher Bandbreite. Hinsichtlich der technischen Implikationen hauptsächlich Funkübertragungen mit kurzer Reichweite. Angedacht als Ersatz für alle Verkabelungen im Computerbereich, wie Monitor, Drucker, etc. Momentan nicht standardisiert. s.a. WiMedia. Working Draft Standard: IEEE 802.15.3a
<<http://www.uwbforum.org>>

V

VoIP Voice over IP

Übertragung von Sprachdaten über IP-Netzwerke. s.a. SIP u. Skype

VoWi Voice over Wi-Fi

Übertragung von Sprachdaten über Wi-Fi-IP-Netzwerke. Im Prinzip identisch mit VoIP.

VPN Virtual Private Network

Direktverbindung eines Clients mit einem VPN-Gateway, das Zugriff auf ein LAN gibt, über ein IP-basiertes Netzwerk, also Erzeugung eines virtuellen LANs. Möglichkeit, die Übertragung zu verschlüsseln.

Standards: IPsec, TLS/SSL, PPTP, L2TP
<http://de.wikipedia.org/wiki/Virtual_Private_Network>
<<http://www.vpnc.org>>

W

WAN Wide Area Network

Netzwerk, das sich über einen großen geographischen Bereich (Kontinente/Länder) erstreckt. Betreiber sind große Unternehmen oder Telco-Provider, die so ihre LANs und MANs verbinden. Das bekannteste WAN ist das Internet.

<http://en.wikipedia.org/wiki/Wide_Area_Network>

WAVE

Wireless Access for the Vehicular Environment

Ergänzung der WLAN-Standards für schnellbewegliche Netzknoten (Autos, Zug, etc.) Standard 802.11p (Draft)

WDS Wireless Distribution System

Standard zur drahtlosen Verbindung von WLAN APs, um größere WLANs aufzubauen. Hierarchischer Aufbau. Roaming möglich. Verschiedene proprietäre Standards. Wird abgelöst durch 802.11s. s.a. Wi-Mesh.

Wearables

Beschreibt die Idee, dass die Computer in die Kleidung integriert sind und diese somit zum tragbaren Computer wird. Heute existieren bereits erste Schritte in diese Richtung, etwa die Integration von Steuerelementen und Verkabelungen in die Kleidung, um Zugriff auf das Mobiltelefon oder den MP3-Player zu haben, obwohl das Gerät irgendwo in der Kleidung verstaut ist.

WEP Wired Equivalent Privacy

Verschlüsselungsverfahren für drahtlose Datenübertragung via IEEE 802.11a,b und g. Basiert auf dem RC4-Algorithmus, der mittlerweile als unsicher gilt. Soll/wird abgelöst von WPA2.

WiBro Wireless Broadband

Funknetzwerkstandard eines koreanischen Industriekonsortiums. In direkter Konkurrenz zu WiMAX und HIPERMAN.
<<http://en.wikipedia.org/wiki/WiBro>>

Wi-Fi Wireless Fidelity

Organisation zu Sicherstellung der Interoperabilität verschiedener Produkte, die auf Basis von IEEE 802.11 Standards arbeiten.
<<http://www.wi-fi.org>>
<<http://www.wi-fi-alliance.org>>
<<http://de.wikipedia.org/wiki/Wi-Fi>>

WiMA Wi-Mesh Alliance

s. Wi-Mesh

WiMAX

Worldwide Interoperability for Microwave Access
Zertifizierungsstelle zur Sicherstellung der Interoperabilität von Funknetzwerken und -technologien verschiedener Hersteller.
Standardset: IEEE 802.16
<<http://www.wimaxforum.org>>
<<http://grouper.ieee.org/groups/802/16/index.html>>
<<http://de.wikipedia.org/wiki/WiMAX>>

WiMedia

Industriekonsortium zur Verbreitung von UWB-Technologien. Auch Wireless USB. Kein unabhängiger Standard bisher final, wegen Streit mit dem UWB-Forum.
Working Draft Standard: IEEE 802.15.3a
<<http://www.wimedia.org>>

Wi-Mesh

Protokoll für Mesh-WLANs. Erarbeitet von der Wi-Mesh Alliance (Philips, Nortel, u.a.). Wird mit SEEMesh im Standard 802.11s aufgehen.
<<http://www.wi-mesh.org>>

WLAN Wireless Local Area Network

Kabelloses IP-Netzwerk mit begrenzter Reichweite. Verschiedene Strukturen (ad-hoc, mesh, etc.) möglich.

Verbreitetste Technologien für WLAN basieren auf dem Standardset IEEE 802.11. Besonderheit ist die Nutzung lizenzfreier (ISM-)Bänder.

<<http://grouper.ieee.org/groups/802/11/index.html>>

<http://www.bundesnetzagentur.de/enid/Allgemeinzuteilungen/WLAN_dv.html>

WLAN AP WLAN Access Point

Knotenpunkt eines WLANs, der den Anschluss an drahtgebundene Netzwerke herstellt, dadurch häufig auch als Internetrouter für das WLAN dient.

WMAN Wireless Metropolitan Area Network

Funknetzwerk, das sich über ganze Regionen oder Städte erstreckt. Besteht aus untereinander vermaschten WLAN Access Points. Aufbau ähnelt Mobilfunknetzen. s.a. MAN.
Standard: IEEE 802.16
<<http://grouper.ieee.org/groups/802/16/index.html>>
<<http://de.wikipedia.org/wiki/WMAN>>

WPA2 Wi-Fi Protected Access 2

Verschlüsselungsstandard für IEEE 802.11a, b und g Funknetze, das auf dem AES basiert. Löst das als unsicher geltende WEP/WPA-Verfahren ab.
Standard: IEEE 802.11i
<<http://wi-fi.org>>

WPAN Wireless Personal Area Network

Nahbereichs-ad-hoc-Kommunikation einzelner Geräte. Drahtgebunden oder auch per Funk, dann aber WPAN genannt. s.a. Bluetooth, NFC und ZigBee
Standardset: IEEE 802.15
<<http://grouper.ieee.org/groups/802/15/index.html>>

WPS Wi-Fi Positioning System

Systeme die zur Positionierung und Lokalisierung dienen auf der Basis von terrestrischen Wi-Fi-Netzwerken, als Konkurrenz zu den Satellitenortungssystemen GPS und Galileo.
<<http://www.skyhookwireless.com>>
<http://www.motorola.com/governmententerprise/northamerica/en-us/public/functions/browsesolution/browsesolution.aspx?navigationpath=id_804i/id_2523i/sso-ne2/sstw013>

WSIS World Summit on the Information Society

Von der ITU organisierte Konferenz, um soziale und politische Belange der globalen Informationsgesellschaft zu diskutieren.

s. Literaturliste: WSIS Golden Book

<<http://www.itu.int/wsis/>>

WUSB Wireless USB

Funkstandard, der Verbindungen zwischen Geräten herstellen soll, als Alternative zum kabelgebundenem USB.

Standard: IEEE 802.15.3a (nicht final). Nicht zu verwechseln mit WirelessUSB™ einem proprietären Standard, der mit Bluetooth vergleichbar ist. s.a. WiMedia und UWB.

<http://en.wikipedia.org/wiki/Wireless_USB>

WWW World Wide Web

Begriff für die Standards und Protokolle, die umgangssprachlich als Internet bezeichnet werden. Die grundlegenden Protokolle und Standards wie HTTP und HTML wurden maßgeblich von Sir Tim Berners-Lee definiert.

Z **ZigBee**

Spezifikation für WPANs nach IEEE 802.15.4. Einsatz als Kommunikationsnetzwerk für Aml. Steht in direkter Konkurrenz zu Bluetooth beziehungsweise ergänzt es als stromsparende Alternative.

<<http://www.zigbee.org>>

<<http://en.wikipedia.org/wiki/ZigBee>>

LITERATURLISTE (GEDRUCKTE PUBLIKATIONEN)

Albrecht, Katherine/McIntyre, Liz:

Spychips – How major corporations and government plan to track your every move with RFID.
Nashville, Tennessee: Nelson Current, 2005.

Becker, Konrad u.a.: *Die Politik der Infosphäre – World-Information.Org, Schriftenreihe Band 386.*
Bonn: Bundeszentrale für politische Bildung, 2002.

Bonsiepe, Gui: *Interface – An Approach to Design.*
Maastricht: Jan van Eyck Akademie, 1999

Brin, David: *The Transparent Society.*
Reading, Massachusetts: Addison-Wesley, 1998.

Burckhardt, Jochen/Henn, Horst/Hepper, Stefan/Rindtorff, Klaus/Schäck, Thomas:
Pervasive Computing – Technologie und Architektur mobiler Internetanwendungen.
München: Addison-Wesley, 2001.

Butler, Jill/Holden, Kritina/Lidwell, William: *Universal Principles of Design.*
Gloucester, Massachusetts: Rockport Publishers, 2003.

Effing, Wolfgang/Rankl, Wolfgang: *Handbuch der Chipkarten, 4. erw. Auflage.*
München: Carl Hanser Verlag, 2002.

Finkenzeller, Klaus: *RFID-Handbuch, 3. erw. Auflage.*
München: Carl Hanser Verlag, 2002.

Garfinkel, Simon (Hrsg.)/Rosenberg, Beth (Hrsg.): *RFID – Applications, Security, And Privacy.*
Addison-Wesley, 2006.

Gershenfeld, Neil: *Wenn die Dinge denken lernen.*
München: Econ Verlag, 1999.

Hansmann, Uwe/Merk, Lothar/Nicklous, Martin S./Stober, Thomas:
Pervasive Computing – The Mobile World, 2. erw. Auflage.
Berlin: Springer Verlag, 2003.

Höger, Hans (Hrsg.)/Burckhardt, Lucius: *Design ist unsichtbar.*
Hatje Cantz Verlag, 1995

Höpfner, Hagen/Türker, Can/König-Ries, Birgitta:
Mobile Datenbanken und Informationssysteme – Konzepte und Techniken.
Heidelberg: dpunkt.verlag, 2005.

Kern, Christian: *Anwendung von RFID-Systemen.*
Berlin: Springer Verlag, 2006.

Khazaeli, Cyrus Dominik: *Systemisches Design*.
Reinbek bei Hamburg: Rowohlt Verlag, 2005.

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

McCullough, Malcolm:
Digital Ground – Architecture, Pervasive Computing, and Enviromental Knowing.
Cambridge, Massachusetts: The MIT Press, 2004.

Norman, Donald A.:
The Design of Everyday Things. New York: Basic Books, 2002.
Emotional Design – Why we love (or hate) everyday things. New York: Basic Books, 2005.

OECD (Hrsg.):
Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,
2002-07.
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2002.
OECD Communications Outlook 2004, 2004.
OECD Communications Outlook 2005, 2005.
RFID Drivers, Challenges and Public Policy Considerations, 2006-02
The Implications of WiMax for Competition and Regulation, 2006-03.
The Promotion of a Culture of Security for Information Systems and Networks in OECD-Countries,
2005-12.
Alle OECD Dokumente sind durch den OECD Publication Service, Paris Cedex, veröffentlicht worden,
und auch als eBooks unter <<http://www.sourceoecd.org>> erwerbbar.

Preece, Jennifer/Rogers, Yvonne/Sharp, Helen:
Interaction Design – Beyond Human-Computer Interaction.
New York: John Wiley & Sons, 2002.

Schnabel, Patrick: *Kommunikationstechnik-Fibel*.
Ludwigsburg: Eigenverlag, 2003.

Schulzki-Haddouti, Christiane (Hrsg.): *Bürgerrechte im Netz, Schriftenreihe Band 382*.
Bonn: Bundeszentrale für politische Bildung, 2003.

Sweeney II, Patrick J.: *RFID for Dummies*.
Indianapolis: Wiley Publishing, 2005.

Thaller, Georg Erwin: *Interface Design – Die Mensch-Maschine-Schnittstelle gestalten*.
Frankfurt: Software & Support Verlag, 2002.

Tufte, Edward R.: *The Visual Display of Quantitative Information*.
Cheshire, Connecticut: Graphics Press, 2004.

LITERATURLISTE (ÖFFENTLICH ZUGÄNLICHE EBOOKS)

Amtsblatt der Europäischen Union:

Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten.

2006-06-06:<http://www.bmi.bund.de/cln_012/Internet/Content/Common/Anlagen/Themen/Informati- onsgesellschaft/DatenundFakten/Biometrie__ePass__EU__VO,templateId=raw,property=publicationFile .pdf/Biometrie_ePass_EU_VO.pdf>

Berthold, Oliver/Günther, Oliver/Spiekermann, Sarah:

RFID – Verbraucherängste und Verbraucherschutz, 2005.

2006-05-06: <<http://www.taucis.hu-berlin.de/~download/rfid.pdf>>

Berthold, Oliver/Spiekermann, Sarah:

Maintaining Privacy in RFID Enabled Enviroments Proposal for a Disable-Model (Privacy, Security and Trust within the Context of Pervasive Computing. Springer Verlag), 2005.

2006-05-07: <http://amor.rz.hu-berlin.de/~spiekers/SPPC_spiekermann-edited.pdf>

Beresford, Alastair R.:

Location Privacy in Ubiquitous Computing, 2005-01.

2006-05-11: <<http://citeseer.ist.psu.edu/cache/papers/cs2/445/http:zSzzSzwww-lce.eng.cam. ac.ukzSzlce-pubzSzpubliczSzarb33zSzUCAM-CL-TR-612.pdf/beresford05location.pdf>>

Bohn/Coroama/Langheinrich/Mattern/Rohs:

Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications. Journal of Human and Ecological Risk Assessment, Vol. 10, No. 5, pp. 763-786, October 2004.

2006-06-06:<<http://www.vs.inf.ethz.ch/publ/papers/hera.pdf>>

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):

RFID - Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, 2004.

2006-05-05:<http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf>

RIKCHA-Studie – Risiken und Chancen des Einsatzes von RFID-Systemen, 2004.

2006-05-05:<<http://www.bsi.de/fachthem/rfid/RIKCHA.pdf>>

Coroama, Vlad/Langheinrich, Marc:

Personalized Vehicle Insurance Rates – A Case for Client-Side Personalization in Ubiquitous Computing. Workshop on Privacy-Enhanced Personalization at CHI 2006, Montréal, Canada, 2006-04-22.

2006-06-06:<http://www.vs.inf.ethz.ch/publ/papers/coroama-langheinrich_2006_client-side-pers.pdf>

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI):

RFID – Funkchips für jede Gelegenheit?, 2004.

2006-05-20:<http://www.bfdi.bund.de/cln_030/nn_531950/SharedDocs/Publikationen/Faltblaetter/ RFIDFunkchipsFuerJedeGelegenheit,templateId=raw,property=publicationFile.pdf/RFIDFunkchipsFuer- JedeGelegenheit.pdf>

ECMA:

Near Field Communication Whitepaper, 2004.

2005-05-05:<<http://www.ecma-international.org/activities/Communications/2004tg19-001.pdf>>

Standard ECMA-340 – Near Field Communication Interface and Protocol (NFCIP-1), 2nd Edition, 2004-12

2005-05-05:<<http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf>>

EICAR:

Leitfaden RFID und Datenschutz, 2006-04-10.

2006-05-20:<<http://www.eicar.org/rfid/infomaterial/RFID-Leitfaden-100406.pdf>>

Eurostat:

Eurostat Jahrbuch 2005, 2005-11.

2006-05-10:<http://epp.eurostat.cec.eu.int/cache/ITY_OFFPUB/KS-CD-05-001/DE/KS-CD-05-001-DE.PDF>

ETSI:

Jahresbericht 2004, 2005-06-06

2006-08-30:<<http://www.etsi.org/etsi%5Fradar/literature/documents/ar%5Fger%5F2004.doc>>

Floerkemeier, Schneider, Langheinrich:

Supporting the Fair Information Practice Principles in RFID Protocols, 2004

2006-06-05:<<http://www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.pdf>>

FOEBUD:

RFID Positionspapier, 2003-11.

2005-05-05:<<http://www.foebud.org/files/positionspapier.pdf>>

Harper, Jim:

RFID Tags and Privacy – How Bar-Codes-On-Steroids Are Really a 98-Lb. Weakling, 2004-06-21.

2006-05-20:<<http://www.cei.org/pdf/4080.pdf>>

i2010:

Erster Jahresbericht über die europäische Informationsgesellschaft, 2006-05.

2006-06-01:<http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/com_2006_215_de.pdf>

ISI & FOKUS (Fraunhofer-Institut für offene Kommunikationssysteme):

Wechselseitiges Verhältnis hochbitratiger Funknetze in künftigen Telekommunikationsmärkten, 2004.

2006-05-05: <<http://bmwi.de/Redaktion/Inhalte/Pdf/S-T/studie-wechselseitiges-verhaeltnis-hochbitratiger-funknetze.property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf>>

ISTAG (IST Advisory Group):

Shaping Europe's Future through ICT, 2006-03.

2006-05-17: <<ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf>>

Ambient Intelligence: From Vision to Reality, 2003.

2006-05-17:<ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf>

ITU:

Internet Reports 2005 – The Internet of Things, Summary.

2006-05-08: <http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf>

Internet Reports 2004 – The Portable Internet, Overview

2006-05-08: <http://www.itu.int/osg/spu/publications/portableinternet/Portableinternetoverview_2004.pdf>

Ubiquitous Computing Privacy Background Paper, 2004

2006-05-08: <<http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf>>

OECD:

Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations.

2006-04-30: <http://www.oecd.org/LongAbstract/0,2546,en_2649_201185_36323192_1_1_1_1,00.html>

Proceedings: Foresight Forum on Radio-Frequency Identification (RFID): Applications and Public Policy Considerations, 2005-10-05.

2006-04-30: <http://www.oecd.org/LongAbstract/0,2546,en_2649_201185_36069214_1_1_1_1,00.html>

Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2005.

2006-04-30: <http://www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html>

The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, 2005.

2006-04-30: <http://www.oecd.org/LongAbstract/0,2546,en_2649_201185_35884542_1_1_1_1,00.html>

Langheinrich, Marc:

RFID and Privacy. In: Milan Petkovic, Willem Jonker (Eds.): *Security, Privacy, and Trust in Modern Data Management*, Springer-Verlag, 2006-07.

2006-06-06: <<http://www.vs.inf.ethz.ch/publ/papers/langhein2006rfidprivacy.pdf>>

Personal Privacy in Ubiquitous Computing – Tools and System Support. PhD thesis No. 16100, ETH Zurich, Zurich, Switzerland, 2005-05.

2006-06-06: <<http://www.vs.inf.ethz.ch/publ/papers/langheinrich-phd-2005.pdf>>

Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. In: Elgar Fleisch, Friedemann Mattern (Eds.): *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis*, Springer-Verlag, 2005.

2006-06-06: <<http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf>>

Siemens/Infrastrat:

Horizons2020 – Ein Szenario als Denkanstoss für die Zukunft, 2004-06

2006-05-20: <http://w3.siemens.de/horizons2020/pdf/inhalt/presse/Horizons2020_Szenariobericht_Komplett.pdf>

Spiekermann, Sarah:

General Aspects of Location Based Services, Kap.1, Location Based Services. Springer Verlag, 2004.

2006-05-07: <http://amor.rz.hu-berlin.de/~spiekers/LBS_9286-Schiller-01.pdf>

SWAMI:

Safeguards in a World of Ambient Intelligence Conference Documentation, 2006-03

2006-06-01: <http://swami.jrc.es/pages/documents/SWAMIConferenceDocumentation_001.pdf>

SWAMI:

Safeguards in a World on Ambient Intelligence Conference Report, 2006-04
2006-06-01: <<http://swami.jrc.es/pages/documents/Deliverable5-ReportonConference.pdf>>

TAUCIS (Hrsg.)/Spiekermann, Sarah:

Auswirkungen des Ubiquitous Computing (UC) auf Verbraucher: Chancen und Risiken, 2006-03.
2006-03-16: <http://www.taucis.hu-berlin.de/_download/TAUCIS_Chancen%20und%20Risiken.pdf>

Weiser, Mark:

The Computer for the 21st Century, in *Scientific American*, S. 94-100, 1991-09.
2006-05-11: <<http://www.stanford.edu/class/cs344a/papers/computer-for-21-century.pdf>>

Zhou:

Intelligent Transportation System - RFID Application (White Paper), 2005
2006-04-30: <<http://www.rfidjournal.com/whitepapers/download/106>>

INTERNETQUELLEN

ALLGEMEINE INFORMATIONEN / PORTALE

- <https://events.ccc.de/congress/2005/wiki/RFID-Zapper>
RFID-Zapper. Zerstören von RFID-Chips, ohne das Trägermaterial zu verletzen.
- <http://www.computer.org/portal/site/pervasive/>
IEEE Pervasive Computing Magazin.
- <http://epp.eurostat.cec.eu.int>
Eurostat – Europäische Statistiken
- http://ec.europa.eu/information_society/text_en.htm
EU Portal Information Society
- http://europa.eu.int/information_society/eeurope/i2010/index_en.htm
EU i2010 Initiative für die europäische Informationsgesellschaft.
- <http://www.heise.de>
News-Portal zu ICT relevanten Themen. Sehr breites Themenspektrum.
- <http://www.heise.de/newsticker/meldung/69127>
heise newsticker: ePass-Kommunikation kann abgehört und geknackt werden.
- <http://www.heise.de/mobil/artikel/68923>
Funknetze stricken. Heise mobil artikel über Meshed Networks.
- <http://www.louisville.edu/library/law/brandeis/privacy.html>
The Right to Privacy – Warren und Lois D. Brandeis, 1890
- <http://www.netstumbler.com/>
News-Portal über Funktechnologien.
- <http://www.rfid-informationen.de>
Private Website zu RFID.
- <http://www.rfidjournal.com>
Webportal des kommerziellen Printmagazin.
- <http://www.rpi-polymath.com/ducttape/RFIDWallet.php>
Anleitung zur Herstellung einer RFID-abschirmenden Geldbörse.
- <http://slashdot.org>
News-Portal zu ICT. Breites Themenspektrum.
- <http://www.wi-fiplanet.com>
News-Portal zu Wi-Fi und anderen Funktechnologien.
- <http://wndw.net/>
Wireless Networking in the Developing World

ANWENDUNGEN VON WMAN/WLAN/NFC/RFID ETC.

- <http://www.europe.nokia.com/nokia/0,,55737,00.html>
Nokia Field Force Solutions (RFID,NFC)
- <http://freifunk.net>
Privat organisierte meshed WLAN-Netze
- <http://www.tfl.gov.uk/tfl/fares-tickets/2006/oyster/general.asp>
Blue Oyster Travelcard Transport for London

<http://www.cclondon.com/>
HP Congestion Charging London.

<http://www.cnut.ws/>
Initiative gegen CCL

<http://www.bbc.co.uk/london/congestion/intro.shtml>
BBC Website über CCL

<http://www.epass.de/>
Informationsübersicht zum deutschen ePass.

http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/ePass__Biometrie/Hintergrundinfo__ePass.html
Hintergrundinformationen zum deutschen ePass.

<http://w3.siemens.de/horizons2020/index.htm>
Horizons2020. Zukunftsszenarien für das Jahr 2020 von Siemens/Infratest.

<http://www.fourthproject.de/mats/>
MATS Mobiles Auskunft- und Ticketing-System – BVG Feldtest

<http://www.future-store.org>
RFID Testsupermarkt der METRO-Gruppe. Future Store Rheinberg

<http://www.mobiloco.de/html/index.jsp>
Mobiloco. Anbieter von Location Based Services für GSM-Netze, wie den Buddy Alert.

http://www.motorola.com/governmentandenterprise/northamerica/en-us/public/functions/browseproduct/productservices.aspx?navigationpath=id_804i
Motorola Communication Networks – MEA™

http://www2.nortel.com/go/solution_content.jsp?segId=0&catId=0&parId=0&prod_id=47160&locale=en-US
Nortel Wireless Mesh Network Solutions

<http://www.philzimmermann.com/EN/zfone/index.html>
Zfone – Verschlüsselung für VoIP, vom PGP-Programmierer.

<http://www.rf-dump.org>
Programm zum Auslesen und Ändern von RFID-Tags. GPL Lizenz.

<http://www.rifid.de>
Analysen und Nachrichten über RFID und UCT.

<http://rmvplus.de> und <http://rmv.erlebniscard.de>
Rhein-Main-Verkehrsverbund Mobiltelefon-Ticketing, get»in-Karte, Erlebniskarte

http://www.sfgov.org/site/tech_connect_index.asp
Übersicht über städtisches "TechConnect" WLAN San Francisco.

<http://www.smartid.gov.hk/en/index.html>
Hong Kong Smart ID Card.

<http://www.telefahrschein.de/>
mPayment mit dem Mobiltelefon im Verkehrsverbund Vogtland.

<http://www.troposnetworks.com>
Metro-scale Mesh Networking.

<http://www.trackyourkid.de/>
Ortungsservice für Mobiltelefone. Richtet sich an Eltern.

KONFERENZEN

<http://www.cfp.org>

Annual Conference on Computers, Freedom & Privacy.

<http://www.i2010.org.uk/>

Die Konferenz zur EU-Initiative i2010, London 2005

<http://www.itu.int/wsis/index.html>

World Summit on the Information Society, Tunis 2005.

<http://www.pervasive2006.org>

Pervasive 2006, Dublin.

<http://cnd.iit.cnr.it/percom2006/>

4th Annual IEEE International Conference on Pervasive Computing and Communications.

<http://www.kierkegaard.co.uk>

LSPI - 1st International Conference on Legal, Security and Privacy Issues in IT, Hamburg.

<http://ubicomp.org>

8th International Conference on Ubiquitous Computing, Orange County.

<http://www.wimaxworld europe.com>

WiMAX World Europe, Wien, 2006. Konferenz und Messe.

DATENSCHÜTZER UND PRIVATSPHÄRENVERFECHTER (WEITERE SIEHE ORGANISATIONEN)

<http://www.foebud.org/rfid>

Stop RFID!-Initiative des Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V, kurz FoeBud.

<http://idtrail.org/>

Gegen Überwachung und für Anonymität im Internet.

<http://www.netzkritik.de>

Blog zu Datenschutz, Internet und UbiCom

<http://www.nocards.org>

CASPIAN - Consumers Against Supermarket Privacy Invasion and Nubering

<http://www.spsychips.com>

Homepage zum Buch. Siehe Literaturliste.

FORSCHUNG & ENTWICKLUNG

<http://www.bsi.de/fachthem/rfid/index.htm>

Bundesamt für Sicherheit in der Informationstechnik Thema RFID -> RIKCHA Studie

<http://www.create-net.org/>

Center of REsearch And Telecommunication Experimentations for NETworked communities

<http://cordis.europa.eu/en/home.html>

CORDIS Community Research & Development Information Service. EU-Informationdienst.

<http://www.disappearing-computer.net/>

EU-Forschungsprojekt zu UC-Anwendungen

http://europa.eu.int/comm/research/fp6/index_en.cfm?p=0_sitemap#FP6home

6. Forschungs-Framework der EU Übersicht.

<http://www-130.ibm.com/developerworks>
IBM Entwicklungsabteilung. Interessant ist Wireless und Architecture.

<http://cordis.europa.eu/ist/istag.htm>
ISTAG. IST Advisory Group. EU-Forschungsprojekt

http://www.ito.tu-darmstadt.de/index_de_html
IT Transfer Office TU Darmstadt

<http://www.inf.ethz.ch/personal/langhein/articles/>
HP Marc Langheinrich, s. Literaturliste

<http://www.cs.ru.nl/paw/>
Privacy in an Ambient World. Niederländisches Forschungsprojekt.

<http://amor.rz.hu-berlin.de/~spiekers/>
HP Dr. Sarah Spiekermann, s.a. TAUCIS.

<http://swami.jrc.es/pages/index.htm>
Safeguards in a World of Ambient Intelligence. EU-Projekt.

<http://www.taucis.de>
Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung

<http://ttd.media.mit.edu/>
Things That Think. MIT Forschungsprojekt.

<http://www.rfidguardian.org/>
Project to develop a privacy and security management device. Andrew S. Tanenbaum u.a.

<http://www.rfidvirus.org/>
Proof-of-Concept für einen RFID-Virus. Andrew S. Tanenbaum u.a.

ORGANISATIONEN

<http://www.autoid.org>
Gegen RFID und andere automatisierte Identifikationssysteme. (NGO)

<http://bmwi.de>
Bundesministerium für Wirtschaft und Technologie

<http://www.car-to-car.org>
Car2Car Communication Consortium, 802.11p

<http://www.cdt.org>
Center for Democracy & Technology (NGO)

<http://www.datenschutzzentrum.de>
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (NGO)

<http://www.eff.org>
Electronic Frontier Foundation (NGO); "Defending Freedom in the Digital World."

<http://www.eicar.org/rfid/>
European Expert Group for IT-Security RFID Task Force

<http://www.epic.org>
Electronic Privacy Information Center (NGO)

<http://www.etsi.org>
European Telecommunication Standards Institute.

<http://portal.etsi.org/radio/sitemap.asp>
Übersicht Funkstandards der ETSI

<http://www.gs1-germany.de>
Gesellschaft von deutschen Handelsorganisationen zur Förderung von RFID/EPC und Verwaltung von EAN

<http://www.intelligentcommunity.org/>
ITF – Intelligent Community Forum. ICT-Entwicklung für Städte.

<http://www.javacardforum.org>
Java für Smartcards und NFC.

<http://www.mobilepaymentforum.org>
Industrieorganisation zur Förderung von mPayment.

<http://www.nfc-forum.org>
Standardisierungsgremien für NFC.

<http://www.okfn.org/wsfii/>
World Summits on Free Information Infrastructures. (NGO)

<http://www.smartcardalliance.org>
Industrieorganisation zur Förderung und Verbreitung von Smartcards.

<http://www.wi-mesh.org>
WiMA – Wi-Mesh Alliance

<http://www.witsa.org>
World Information Technology and Services Alliance (NGO)

