Aus: Friedemann Mattern (Hrsg):
Die Informatisierung des Alltags –
Leben in smarten Umgebungen, 2007

Gibt es in einer total informatisierten Welt noch eine Privatsphäre?

Marc Langheinrich
Institut für Pervasive Computing, ETH Zürich

But lo! Men have become the tools of their tools. Our inventions are wont to be pretty toys which distract our attention from serious things.
Henry David Thoreau

Kurzfassung. Die Vision allgegenwärtiger, „intelligenter" Umgebungen nährt die Angst vor einer umfassenden Überwachung des Einzelnen durch Staat und Wirtschaft sowie vor dem Missbrauch durch Kriminelle. Sind solche Ängste eher unbegründet, da zwischen Vision und Realität immer noch technische, soziale und rechtliche Machbarkeiten Grenzen ziehen? Oder bewegen wir uns mehr oder weniger zwingend hin in Richtung einer Gesellschaft, in der es ganz normal sein wird, dass praktisch all unsere Handlungen und Bewegungen aufgezeichnet und in digitalisierter Form für andere abrufbar sein werden? Dieser Beitrag versucht, anhand gesellschaftlicher Trends und Begehrlichkeiten Entwicklungspotenziale aufzuzeigen, die sich durch die Bereitstellung „smarter" Technik ergeben. Dabei sollen gezielt deren Risiken und Herausforderungen angesprochen werden, die sowohl in technischer, vor allem aber auch in gesellschaftlicher Hinsicht auftreten. Ob wir unter diesen Umständen auch in Zukunft noch eine umfassend geschützte Privatsphäre haben werden, wird mehr denn je davon abhängen, welchen Wert unsere Gesellschaft diesem Gut beim Abwägen gegenüber Bequemlichkeit, Effizienz und Sicherheit zuweisen wird.

Einleitung

Während Aktivistenorganisationen wie der Bielefelder FoeBud[1] oder die amerikanische CASPIAN[2] immer wieder äußerst erfolgreich öffentlichen Druck gegen aktuelle Datenerhebungsprojekte großer Handelsketten aufbauen, erfreut sich die ubiquitäre Kundenkarte weiterhin großer Beliebtheit: Eine Emnid-Umfrage im März 2002 fand über die Hälfte der befragten Deutschen im Besitz mindestens einer Kundenkarte [Emn02b], auf eine große Anfrage der FDP im Deutschen

[1] FoeBud heißt mit ganzem Namen *„Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V."*, siehe www.foebud.org.

[2] CASPIAN steht für *„Consumers Against Supermarket Privacy Invasions and Numbering"*, siehe www.nocards.org und www.spychips.com.

Bundestag im Februar 2005 hin schätzte die Bundesregierung sogar über 70 Millionen ausgegebene Rabatt- und Kundenkarten [Bun05]. Gleichermaßen unterschiedlich fallen Beurteilungen bezüglich der Praxistauglichkeit der visionären, „allgegenwärtigen" Technologien aus: Noch 2002 beklagten führende Forscher auf dem Gebiet des Ubiquitous und Pervasive Computings die mangelnde Praxisrelevanz ihrer Prototypen [DaG02] – dem stehen im Jahr 2006 über drei Millionen ausgegebener Eintrittskarten mit personalisierten RFID-Chips zur Fußball-Weltmeisterschaft in Deutschland und einige hunderttausend seit November 2005 ausgegebene biometrische deutsche Reisepässe mit integriertem RFID-Chip gegenüber.

RFID-Funketiketten sind längst nicht das Einzige, was die Forschung in diesem Bereich zu bieten hat. Doch aufgrund ihres relativ hohen „Alters" (erste RFID-Chips wurden bereits in den 1970er Jahren erprobt [AIM01]) hat RFID als eine der ersten Ubiquitous-Computing-Technologien die Anfangshürde des „Technik-Hype-Cycles" [Gar95] überschritten und setzt nun zum Sprung zur Etablierung im Alltag an. Es ist dieser „*move into the everyday*", den Mark Weiser in seinem wegweisenden Artikel „The Computer for the 21st Century" [Wei91] als Kennzeichen einer neuen Art von Computersystemen ausmachte, die unauffällige Einbettung von Technologie in Alltagsgegenstände und -handlungen, bei der das Bewusstsein für die Verwendung eines Computers praktisch verschwindet. Schon Weiser war der zweischneidige Charakter solch einer Entwicklung bewusst – die unauffällige Beobachtung durch Computersysteme ermöglicht

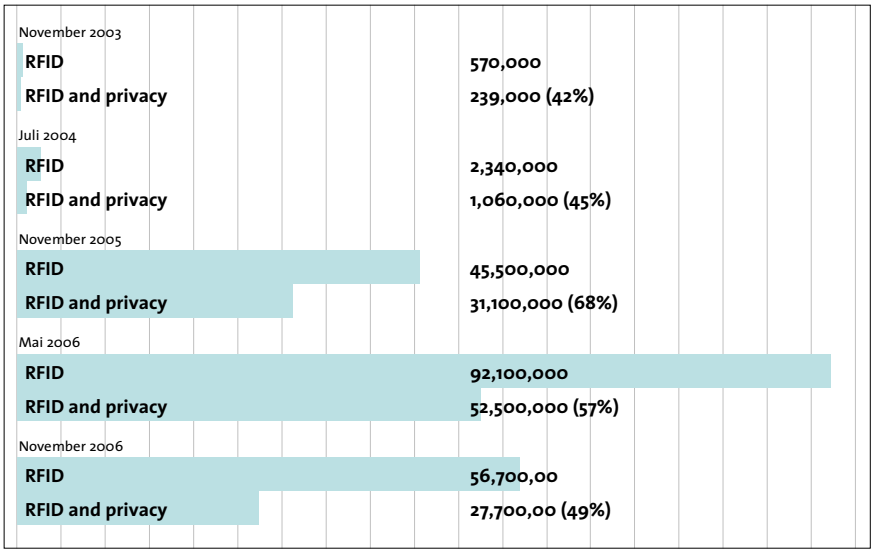

Abb. 1. RFID und Datenschutz (*privacy*) im öffentlichen Bewusstsein (gemäß Google-Index): Im Frühjahr 2006 wurde das Nischenprodukt „Funketikett" zum globalen Thema mit über 90 Millionen Treffern im Google-Index. Inzwischen ist das Interesse offenbar wieder zurückgegangen, doch fallen Ende 2006 immer noch knapp die Hälfte aller Nennungen im Zusammenhang mit Datenschutzaspekten.

ein neues Paradigma des „Calm Computings“, während gleichzeitig die Möglichkeiten zur unbemerkten Überwachung steigen – doch hatte er bereits einen Lösungsansatz parat: *„The problem, while often couched in terms of privacy, is really one of control“* [Wei99]. Das Ausloten von Möglichkeiten, die Kontrolle darüber zu behalten, wer wann und zu welchem Zweck von mir mitgeführte Funketiketten ausliest (immer vorausgesetzt, ich bin mir darüber überhaupt im Klaren, *dass* ich solche bei mir trage), gehört mit zu den aktivsten Forschungsfeldern der RFID-Technologie [Lan05b, Lan07]. Doch während das Interesse an RFID und vor allem die Besorgnis über dessen Überwachungspotenzial steigen (siehe Abb. 1), schreitet die Verbreitung der Miniaturcomputer scheinbar ungehindert voran: Laut einer Studie des Technologieberatungskonzerns Gartner wurden 2005 weltweit mehr als eine halbe Milliarde US-Dollar für RFID-Systeme ausgegeben [TMC05] (ein Zuwachs von knapp 40% zum Vorjahr); fast jeder fünfte Hersteller, Logistiker und Händler hatte konkrete Pläne, erste Pilotprojekte oder bereits laufende Systeme im Einsatz [IDC06].

Ist die flächendeckende Verbreitung des Ubiquitous Computings also bereits abzusehen? Ist der heutige Einsatz von RFID überhaupt ein Indiz für die Etablierung der viel weiter reichenden Vision einer „intelligenten“ Umgebung? Und führt diese Vision unweigerlich zu den oft beschworenen Überwachungsdystopien im Stil von Orwells *1984*? Im Folgenden soll, ausgehend von heutigen Entwicklungen und Trends, versucht werden abzuschätzen, inwieweit sich die Technologien des Ubiquitous Computings in unserem Alltag etablieren und dadurch unsere Privatsphäre beeinflussen werden. Auch wenn konkrete Aussagen über die Zukunft oft schwierig, wenn nicht gar unmöglich erscheinen, kann eine solche Betrachtung womöglich das Bewusstsein für die Problematik schärfen und Handlungszwänge aufzeigen, die in Folge einer „informatisierten“ Gesellschaft [Mat03] auf uns zukommen.

Effiziente Produktion und Vertrieb

Nicht erst seit Globalisierung und hohe Arbeitslosigkeit Schlagzeilen machen, ist wirtschaftliche Effizienz ein Thema. Der Einsatz ubiquitärer Technologien, d.h. vor allem die Nutzung von RFID-Funketiketten, verspricht nun aber signifikante Kosteneinsparungen nicht nur in der Lagerhaltung, sondern auch in vielen Produktionsprozessen.[3] Einzelhandelsgigant Wal-Mart schreibt bereits seit Anfang 2005 seinen hundert größten Zulieferern die Verwendung von Funketiketten auf Paletten und Verpackungseinheiten vor[4] – ersten Auswertungen zufolge konnte dadurch für viele Produkte die „Out-of-Stock“-Quote um bis zu 62% reduziert werden [Col06], was sich beispielsweise bei Rasierklingen von Gillette in einer Umsatzsteigerung von 19% niederschlug [Das06]. Ähnliche Erfolge melden die

[3] Zur Theorie des Bull-Whip-Effektes siehe z.B. [FlM05].

[4] Inzwischen setzen die 300 größten Wal-Mart-Zulieferer RFID auf Paletten und Verpackungseinheiten ein [Das06].

deutsche Metro und der britische Einzelhändler Tesco, die ebenfalls RFID-Technologie in einigen ihrer Verteilzentren einsetzen [Ren06]. Getreu dem Motto *„You can't control what you can't measure"* [DeM86] helfen hier ubiquitäre Technologien, Produktions- und Warenflüsse immer detaillierter und nahezu in Echtzeit verfolgen zu können.

Die Möglichkeit, mittels drahtloser Identifikationstechnologie, integrierter Sensorik und fortschreitender Miniaturisierung betriebliche, industrielle und ökonomische Prozesse immer feingranularer überwachen und steuern zu können, wird nach Ansicht des britischen Nachrichtenmagazins *The Economist* die durch das Internet aufgekommene „New Economy" ablösen und den Übergang zur „Now Economy" einleiten: *„Many companies will use information technology to become a ‚real-time enterprise' – an organisation that is able to react instantaneously to changes in its business"* [Eco02]. Dass hier nicht bei Paketen und Ersatzteilen haltgemacht wird, zeigen aktuelle Entwicklungen in den USA, wo das detaillierte Überwachen und Überprüfen von Angestellten bei vielen Arbeitgebern längst die Regel ist: In einer Studie aus dem Jahr 2000 überwachten knapp drei Viertel aller großen US-amerikanischen Arbeitgeber die Arbeit ihrer Angestellten regelmäßig mit Hilfe von Telefon- und Videoaufzeichnungen bzw. E-Mail- und Internet-Überwachung [SoR03].[5] Mit Technologien des Ubiquitous Computing kann die betriebliche Überwachung leicht jenseits des PCs ausgeweitet werden. Schon heute setzen viele Firmen GPS-basierte Ortungssysteme in ihrem betrieblichen Fuhrpark ein, um nicht nur die kurzfristige Disposition der Mitarbeiter zu erleichtern, sondern auch deren Pausen und Tagesabläufe überprüfen zu können.[6] Sicherheitsfirmen verwenden bereits seit Jahren elektronische Wegmarken um sicherzustellen, dass Wachmänner auch wirklich zur vorgeschriebenen Zeit die vorgesehene Runde drehen, indem diese, wie bei einer Schnitzeljagd, die Marker nach und nach mit einem mobilen Gerät abscannen. Die in Cincinnati im US-Bundesstaat Ohio ansässige Videoüberwachungsfirma CityWatcher hat im Februar 2006 dieses Prinzip sogar umgedreht und lässt ihren Mitarbeitern einen Mikrochip unter die Haut implantieren, der nun seinerseits von an neuralgischen Punkten angebrachten Sicherheitsscannern überprüft werden kann [Hei06].[7]

---

[5] Dabei gibt es durchaus nachvollziehbare Gründe für diesen Trend in einem Land, in dem Arbeitgeber schnell mit Millionenklagen rechnen müssen: nicht nur wenn die Sicherheit anderer auf dem Spiel steht (z.B. bei Zug-, Bus- oder Lastwagenführern, Piloten und Mechanikern, aber auch etwa bei Kinderbetreuung), sondern auch, um die Sicherheit und Qualität des Arbeitsplatzes selbst (Stichwort: *sexual harassment*) zu gewährleisten.

[6] Ein einschlägiger Anbieter solcher Systeme bewirbt sein Produkt mit „Damit Ihr Fuhrpark nicht länger ein ‚schwarzes Loch' ist und die entscheidenden Stellen exakt wissen, WER mit WELCHEM Fahrzeug WAS macht und sich WO und WIE bewegt (hat)", siehe www.telematikteam.de.

[7] Sicherheitsexperten sind sich allerdings einig, dass dadurch die Sicherheit eher gesunken ist: Der von der Firma verwendete „VeriChip" (siehe www.verichipcorp.com) verfügt über keinerlei Sicherheitsmerkmale, die ein unerwünschtes Auslesen und Kopieren verhindern würden: *„The Verichip is a repurposed dog tag; there is no reason (counterfeit housepets?) why it would have been designed with any security features, and in fact it was not"* [Wes05].

Der Einfluss betrieblicher Überwachungssysteme auf die Privatsphäre des einzelnen Konsumenten darf dabei nicht unterschätzt werden: Die RFID-Investitionen der großen Vorreiter Wal-Mart, Tesco und Metro (sowie auch des US-amerikanischen Verteidigungsministeriums, eines der größten Logistikunternehmen weltweit) helfen auf breiter Front, die Kosten zu senken sowie Know-how aufzubauen, was wiederum die Verbreitung von RFID auch im kleineren Maßstab begünstigt. So sind beispielsweise in allen 69 Samsung-Tesco-Supermärkten[8] in Korea sämtliche Einkaufswagen und -körbe mit RFID-Tags ausgestattet, mit denen die Bewegungen der Kunden innerhalb eines Marktes verfolgt werden [Tan06]. Angeblich wurden anhand dieser Daten bereits in einigen Märkten erfolgreich Produktstandorte relokalisiert.[9] Ebenso haben bereits mehrere große öffentliche Bibliotheken (Wien, Graz, Winterthur, München, Stuttgart, selbst im Vatikan) Funketiketten in ihre Bücher integriert, um sowohl die Inventur als auch den Ausleihprozess zu optimieren [ThG05, Kan04]. Und Firmen, die Überwachungssoftware für den PC-Arbeitsplatz entwickeln, bieten inzwischen in vielen Fällen ähnliche Produkte für Schulen, Bibliotheken und besorgte Eltern an.[10] Infrastrukturen für RFID und lokalisierbare, drahtlose Funksender stellen also quasi eine Art „Einstiegsdroge“ in die schöne neue Welt des Ubiquitous Computings dar: Die Kosten sind inzwischen niedrig genug, das technische Know-how bei einer Reihe von Ingenieurbüros vorhanden und die realisierbaren Einsparungen oft signifikant.

Doch neben Effizienzgewinnen versprechen die neuen Kontrollmöglichkeiten ubiquitärer Technologien auch einen wirtschaftlichen Vorteil ganz anderer Art: die Bindung von Kunden an Produkte bzw. den Einsatz dieser Produkte in vom Hersteller gewünschten Bahnen. Im Rahmen der *Trusted Computing Platform Alliance*, die später in *Trusted Computing Group*[11] umbenannt wurde, arbeiten zum Beispiel namhafte Computerhersteller bereits seit 1999 an einer Architektur, die zur Erhöhung der IT-Sicherheit ein Manipulieren von Daten und Software auf Computern verhindern soll. Dazu versehen Hersteller ihre Programme (bzw. Bilder, Videos oder Musikstücke) mit einer digitalen Signatur, die dann ein neu in PCs verbauter Chip – das sogenannte *Trusted Platform Module* – auf Echtheit prüfen kann [Him03]. Während Befürworter des *Trusted Computings (TC)* auf die neuen Möglichkeiten verweisen, mit dieser Architektur Viren und Spyware zu verhindern (die als nicht signierte Programme gar nicht oder nur sehr eingeschränkt lauffähig wären), warnen prominente Kritiker wie Richard Stallman[12]

[8] Samsung-Tesco-Supermärkte sind ein Joint Venture zwischen dem Elektronikriesen Samsung und dem britischen Einzelhändler Tesco.

[9] Dies steht im Gegensatz zum modernen „Beer and Nappies“-Märchen, dass Wal-Mart angeblich dank Data Mining eine hohe Korrelation zwischen Bier- und Windelkäufen erkannt haben soll und durch cleveres Umplatzieren der entsprechenden Produktgruppen Millionengewinne einfahren konnte [Bis06, Fri97].

[10] Siehe zum Beispiel www.spectorsoft.com.

[11] www.trustedcomputinggroup.org

[12] Richard Stallman ist Mitbegründer des GNU-Projekts und einer der Vorreiter der „Freien Software-Bewegung“. Seine Homepage findet sich auf www.stallman.org.

oder Ross Anderson[13] vor einer Vision des *Treacherous Computings*, in der statt des PC-Besitzers nun nur noch die Hersteller von Betriebssystemen und PC-Hardware die Kontrolle darüber besitzen, welche Programme und Operationen vom Computer ausgeführt werden können [Sta06, And03].

Dass sich die Konzepte des „Trusted" oder „Treacherous" Computings in Zukunft auch in der realen Welt umsetzen lassen, zeigen bereits erste „smarte" Produkte. So statten bereits heute die Druckerhersteller Epson und Canon ihre Tintenkartuschen mit Überwachungschips aus, welche nicht nur Drittherstellern den Nachbau kompatibler Alternativprodukte erschweren, sondern darüber hinaus unabhängig vom Füllstand der Patrone nach einer bestimmten Zahl von Ausdrucken ein Auswechseln der Kartusche erzwingen (und damit ein kostengünstiges Wiederbefüllen verhindern) [Sch06a].[14] Ähnliche „Lock-in"-Effekte versprechen sich Automobilhersteller und deren Zulieferer von der Nutzung von RFID im Ersatzteilehandel, bei dem Kunden beim Kauf von (RFID-getaggten) Originalteilen zunächst z.B. längere Garantiezeiten gewährt werden könnten [Det06], aber ähnlich wie Tintenpatronen schlussendlich nur noch Originalteile (mit Chip) ordnungsgemäß funktionieren würden.[15]

Effizienz, Produkt- und Betriebssicherheit sowie die Wahrung von Absatzmärkten sind also bereits heute Kernfaktoren einer global im Wettstreit stehenden Wirtschaft. Mit der fortschreitenden Globalisierung werden solche Aspekte eher noch an Bedeutung gewinnen und somit in Zukunft immer wichtigere Gründe für den verstärkten Einsatz ubiquitärer Technologien liefern. Firmen, die Einkauf, Produktion, Vertrieb und Absatz ihrer Produkte minutiös überwachen und dadurch steuern können, werden über einen entscheidenden Wettbewerbsvorteil verfügen, der sich nur durch die konsequente Verwendung von RFID-Chips, Sensorplattformen und drahtlose Vernetzung aufrecht erhalten lassen wird. Und mit wachsenden Absatzmärkten fallen die Kosten der Technologie bei steigendem Know-how für die praktische Umsetzung – die Grundvoraussetzungen für den erfolgreichen und rentablen Einsatz solcher Technik in zahllosen Bereichen, auch außerhalb primär industrieller Interessen. Denn auch wenn Kunden indirekt durch günstigere Preise von dem Effizienz steigernden Einsatz ubiquitärer Technik

[13] Ross Anderson ist Professor für Computersicherheit an der Cambridge University und ein bekannter Sicherheitsexperte. Seine Homepage ist www.cl.cam.ac.uk/~rja14.

[14] Dies hat wiederum zum Aufkommen spezieller Wiederbefüllfirmen geführt, die beim kostengünstigen Recycling einer Patrone auch gleich die eingebauten Chips neu programmieren.

[15] Eine nicht weniger invasive Art der Kontrolle stellt das im Juli 2005 vom obersten Gericht des kanadischen Bundestaates British-Columbia verhängte „Leseverbot" dar, nachdem aus Unachtsamkeit ein Buchladen vierzehn Exemplare des neuesten Harry-Potter-Romans einige Tage vor dem offiziellen Verkaufsstart am 16. Juli verkauft hatte. Auch wenn die Käufer die Bücher rechtmäßig erworben hatten, so wurde ihnen vom Gericht das Lesen des Werkes (bzw. dessen Weiterverkauf) vor dem 16. Juli verboten. Ein Medienrechtswissenschaftler bemerkte trocken: „*There is no human right to read*" [MaC05]. Mit elektronischen Büchern (eBooks) oder elektronischem Papier (eInk) hätte der Verleger die verkauften Exemplare einfach aus der Ferne sperren können.

profitieren können, so sind es natürlich zuallererst Hersteller und Händler, die mit solch einer detaillierten Erfassungs- und Steuerungsmöglichkeit Kosten einsparen bzw. Vertriebskanäle sichern können. Eine wichtige Bedeutung bei der Abschätzung des zukünftigen Einsatzes ubiquitärer Technik kommt deshalb auch Anwendungen zu, welche dem Endkunden einen *direkten* Nutzen versprechen. Diese sollen im nächsten Abschnitt näher betrachtet werden.

Bequemlichkeit und Komfort

Auch wenn der Einsatz von Ubiquitous Computing in Industrie und Handel immer populärer werden sollte – Beispiele wie die öffentliche Diskussion um den Einsatz von RFID in Metros *Future Store* scheinen darauf hinzuweisen, dass Kunden sich bei einer lediglich Herstellern und Händlern zugute kommenden Technologie schnell ausspioniert und ausgenutzt vorkommen können. Dennoch scheint es verfrüht, aus der bisher überwiegend kritischen Berichterstattung zum Thema RFID ein generelles Problem bei der Einführung ubiquitärer Technik in unserem Alltag ausmachen zu wollen. Denn jenseits smarter Supermärkte stehen zahlreiche RFID-basierte Anwendungen bereits seit Jahren hoch in der Gunst der Kunden, offenbar ohne irgendwelche Datenschutzdebatten zu provozieren. So werden bereits seit 1995 alle Neuwagen in Deutschland nur noch mit einer elektronischen Wegfahrsperre ausgeliefert [VDA99], bei der ein im Autoschlüssel integrierter RFID-Chip von einem am Zündschloss angebrachten Lesegerät beim Starten des Motors ausgelesen wird und nur bei korrekter Identifikation des Schlüssels die Motorelektronik freigegeben wird. Seit der Einführung dieser Technologie sind alleine in Deutschland die Diebstahldelikte bei Neuwagen um mehr als 80% zurückgegangen [VDA06]. Ähnlich beliebt sind schlüssellose Zugangssysteme im Automobilbereich, bei denen das Auto auf Knopfdruck ver- und entriegelt werden kann,[16] bzw. lediglich eine Chipkarte mitgeführt werden muss, um den Wagen automatisch zu- und aufzuschließen.[17]

Ebenfalls im automobilen Umfeld haben sich in vielen Ländern RFID-basierte Zahlungssysteme etabliert, wie beispielsweise der italienische TELEPASS[18] oder der US-amerikanische *Exxon Speedpass*[19]. Das TELEPASS-System erlaubt bereits seit 1989 Autofahrern auf italienischen Autobahnen, Mautstellen ohne Anhalten zu passieren. Beim Durchfahren der speziellen TELEPASS-Spuren identifiziert die Mautstation den vorbeifahrenden Wagen mittels eines im Auto befindlichen

[16] Im Gegensatz zur elektronischen Wegfahrsperre operieren diese Systeme jedoch nicht mit RFID-Chips, sondern senden batteriegetrieben per Funk oder Infrarot verschlüsselte Impulse aus.

[17] Antennen innerhalb des Wagens können dabei sicherstellen, dass sich die Chipkarte beim Starten des Motors auch wirklich im Auto befindet.

[18] www.telepass.it

[19] www.speedpass.com

batteriegetriebenen Geräts[20] und erstellt im Dreimonatsrhythmus eine detaillierte Rechnung. Ähnliche Systeme gibt es inzwischen weltweit, z.B. in den USA (EZ-PASS[21] im Nordosten, SunPass[22] in Florida oder TxTAG[23] in Texas), Japan (ETC[24]) oder Hong Kong (Autotoll[25]). Die Zahl der freiwilligen Nutzer solcher Systeme steigt in vielen dieser Länder jährlich weiterhin im zweistelligen Prozentbereich: So gab es Anfang 2006 beispielsweise über 4,9 Millionen TELE-PASS-Nutzer in Italien [ASE06], etwa 15% mehr als noch Anfang 2005 [ASE05].

Ähnlich populär, mit über 8 Millionen Nutzern weltweit [Exx05], ist der vom Ölmulti ExxonMobil seit 1997 vertriebene *Speedpass*, der ein bargeldloses Tanken und Einkaufen an allen US-amerikanischen Exxon- und Mobil-Tankstellen erlaubt, indem ein am Schlüsselbund angebrachter RFID-Chip beim Auflegen auf ein spezielles *Speedpass*-Feld an Zapfsäule bzw. Kasse die persönlichen Zahlungsinformationen des Kunden (z.B. dessen Kreditkartennummer) übermittelt.[26] Weniger universell nutzbar, dafür aber nicht weniger beliebt, sind auch die weltweit in vielen Skigebieten eingesetzten kontaktlosen Skipässe: Statt Streifenkarten, die erst mühsam vom Liftpersonal abgeknipst werden müssen, oder Magnetkarten, die man in kleine Schlitze am Lifteingang einführen muss und die dazu ein umständliches Ausziehen der Handschuhe bzw. ein Suchen nach der richtigen Anoraktasche nötig machen, erlauben auf RFID-Tags geladene Skipassinformationen ein unkompliziertes Überprüfen der Skipassgültigkeit durch die Jackentasche hindurch. Das in einige Swatch-Uhren eingebaute *Snowpass/Access* System[27] ermöglicht sogar das Speichern von Tages-, Wochen- und Saisonkarten auf der eigenen Armbanduhr, zum Teil sogar bequem vor der Anreise ins Skigebiet vom heimischen PC aus. Allein die österreichische Firma SKIDATA[28] hat weltweit über 500 Skigebiete mit solchen Systemen ausgestattet.

Die obigen Beispiele deuten darauf hin, dass ein Einsatz ubiquitärer Technologie zur effizienteren Durchführung altbekannter Vorgänge, d.h. sowohl im eigentlichen Ablauf, als auch in der dazu nötigen Vorbereitung, mit hohen Akzeptanzraten bei Konsumenten rechnen kann. So könnten reparaturanfällige Haushaltsgeräte wie Kaffee-, Wasch- und Geschirrspülmaschinen eine unkomplizierte Garantieabwicklung dank RFID-basierter Identifikation durch den Kundendienst bieten.

---

[20] Dazu wird ein für den automobilen Einsatz entwickeltes RFID-Protokoll namens *Dedicated Short Range Communications* (DSRC) verwendet.

[21] www.ezpass.com

[22] www.sunpass.com

[23] www.txtag.org

[24] www.go-etc.jp (in Japanisch)

[25] www.autotoll.com.hk/en/main.php

[26] Zwar haben Forscher an der US-amerikanischen Johns-Hopkins-Universität im Februar 2005 die lediglich 40-bit starke Verschlüsselung des dem Speedpass zugrunde liegenden RFID-Chips – dem Texas Instruments DSG Tag – brechen können [BGSJ+05], doch hält Hersteller Texas Instruments solche Angriffe für kaum praktikabel [Rob05].

[27] www.swatch.com/snowpass

[28] www.skidata.com

Mit der zunehmenden Verbreitung von sogenannten NFC-fähigen[29] Mobiltelefonen, die RFID-Tags auslesen können, sind sogar Selbstdiagnosesysteme denkbar, bei denen der Kunde sein Handy an das defekte Gerät hält und die Fehlerursache übermittelt bekommt, um entweder ein fehlendes Ersatzteil direkt im Herstellershop bestellen zu können bzw. den Besuch eines Servicemechanikers zu vereinbaren [Rod06].

Überhaupt könnte die NFC-Technologie das Mobiltelefon in Zukunft mehr denn je zum zentralen Bestandteil des modernen Lebens zu machen. So erproben bereits seit geraumer Zeit mehrere Verkehrsverbünde in Europa in groß angelegten Feldversuchen den Einsatz NFC-basierter Fahrkartensysteme. Realität ist dies bereits in Japan, wo Handybesitzer beim Eintreten bzw. Verlassen der U-Bahn-Station nur kurz ihr Handy an das Drehkreuz halten, um automatisch den korrekten Fahrpreis zwischen Ein- und Ausstiegsort abgebucht zu bekommen [Wik06a]. In Hanau bei Frankfurt/Main kann seit April 2006 in sämtlichen Stadtbussen per NFC-Handy bezahlt werden – nach einem zehnmonatigen Feldversuch mit über 150 Kunden stieß dieses Angebot auf so viel Begeisterung, dass es praktisch übergangslos im Regelbetrieb eingesetzt wurde. Der Besitzer eines entsprechenden Mobiltelefons hält beim Ein- und Aussteigen das Handy einfach in die Nähe des im Bus angebrachten Lesegerätes und erhält zum Monatsende eine Rechnung, in der sämtliche unternommene Fahrten mitsamt den Kosten aufgeführt sind [CoN06].

Bei all diesen Beispielen geht es nicht nur um die durch den Einsatz von moderner Technik *unmittelbar* eingesparte Zeit – das schnellere Durchfahren der Maut- oder Liftstation, das schnellere Abschließen des Autos oder das einfache Bezahlen durch „Handy-Auflegen“. Auch der indirekte, d.h. durch Vorbereitung und Unterhalt nötige Aufwand kann für den Nutzer moderner Technik einen signifikanten Anstieg der Bequemlichkeit – und damit implizit eine hohe Akzeptanz trotz potenzieller negativer Seiteneffekte – bedeuten. Bestes Beispiel ist das Mobiltelefon, welches im eingeschalteten Zustand dem jeweiligen Mobilfunkbetreiber (bzw. im Falle eines Verbrechens den Strafverfolgungsbehörden) ein praktisch lückenloses, weltweites Bewegungsprofil des Kunden liefert. Doch der Vorteil, schnell und unkompliziert überall und jederzeit Termine umzudisponieren bzw. Auskünfte einholen zu können, wiegt offensichtlich für viele Nutzer die Nachteile einer potenziellen Überwachung mehr als auf. Gleiches gilt für die Errungenschaft des bargeldlosen Bezahlens durch Geld-, Bank- und Kreditkarten, die den kartenausgebenden Instituten detaillierte Einblicke in die Kauf- und Bewegungsmuster der Kunden erlauben.[30] Doch angesichts ihrer substantiellen Vorteile (keine umständliche Suche nach Kleingeld, Bankautomat oder Wechsel-

[29] Die Abkürzung NFC steht für *Near Field Communication* und bezeichnet einen herstellerübergreifenden Standard, der es z.B. Mobiltelefonen erlaubt, spezielle NCF-kompatible Funketiketten drahtlos auszulesen.

[30] Mit der zunehmenden Verbreitung von NFC-fähigen Mobiltelefonen werden schließlich nicht nur Kommunikations- und Bewegungsmuster, sondern auch die persönlichen Kaufmuster zentral verfolgbar sein.

stube) werden die „Gefahren“ für die persönliche Privatsphäre nüchtern abgewogen und in den meisten Fällen als akzeptabel beurteilt.

Man kann einwenden, dass die Überwachung durch Kreditkarte oder Mobiltelefon sich insofern von der Gefährdung durch RFID und Ubiquitous Computing unterscheidet, als dass hier nur einige wenige, mit speziellen (und teuren) Geräten ausgestattete Firmen (bzw. über den Rechtsweg auch Polizei und Gerichte) Zugriff auf die bei der Verwendung entstehenden Bewegungsmuster haben. Sollten RFID-getaggte Produkte und Miniatursensortechnologie Einzug in unser tägliches Leben finden, so stände es plötzlich praktisch jedem offen, für wenige hundert Euro die nötige Ausrüstung zu besorgen, um Kunden, Nachbarn oder Angestellte auszuspionieren. Aus der hohen Akzeptanz für Mobiltelefone und bargeldloses Zahlen könne also kaum auf eine positive Einstellung gegenüber ubiquitärer Technologien im Allgemeinen geschlossen werden. Doch auch hier zeigt bereits heute der Markt, wie annehmbar solche Überwachungssysteme in privater Hand sein können. Vorreiter ist die US-amerikanische Firma Wherify Wireless, die bereits 2002 eine spezielle Kinderuhr auf den Markt brachte, mit der besorgte Eltern auf Knopfdruck den momentanen Aufenthaltsort ihres Kindes abrufen konnten [Sch02a]. Gerade wenn es um den Schutz von Kindern geht, scheint der Glaube an den Segen der ubiquitären Technik scheinbar unbegrenzt. So sollen bereits mehrere zahlungskräftige Kunden im entführungsgefährdeten Lateinamerika ihr Interesse an implantierbaren RFID-Chips bekundet haben, in der Hoffnung, dadurch im Entführungsfall leichter auffindbar zu sein [Sch02b, Haf06]. Nach einer Serie von Kindesentführungen in Großbritannien meldeten sich dutzende besorgter Eltern bei Kevin Warwick – ein für seine spektakulären Selbstversuche bekannter Professor für „Kybernetik“ an der Universität Reading – mit der Bitte, ihre Kinder mittels eines unter der Haut injizierten RFID-Chips ortbar zu machen[31] – obwohl nach Meinung von Experten die dazu verwendete Technologie kaum in der Lage ist, ein entführtes Kind zu orten [Let02].[32]

Inzwischen haben auch zahlreiche Mobilfunkbetreiber ähnliche Angebote im Programm, vor allem in Japan, wo bereits mehr als 20% aller Mobiltelefone GPS-Lokalisation eingebaut haben [Eur05].[33] In Deutschland bietet die Firma jackMobile[34] mit *track-your-kid*, *track-your-truck* und *track-your-handy* mehrere Dienste zum Auffinden verlorengegangener Kinder, Fahrzeuge bzw. Mobiltelefone [Mat05]. Selbst in den in der Mobilfunktechnologie eher etwas rückständigen

[31] Eine Bitte, der Warwick eigenen Angaben zufolge nur zu gerne nachkommen würde (da er vom Erfolg einer solchen Maßnahme überzeugt ist), die er aber aufgrund der negativ aufgeheizten Diskussion in der Presse bisher ablehnen musste [War06].

[32] Selbst wenn es in Zukunft injizierbare Peilsender geben sollte, wären sie aufgrund ihres Aufbaus natürlich auch für die Entführer leicht am Körper des Kindes zu lokalisieren – und damit etwa durch Herausschneiden zu entfernen. Nach kurzer Zeit würden Entführungen womöglich also blutiger ablaufen als je zuvor.

[33] So bietet beispielsweise KDDI das GPS-basierte „EZ-Navi“ System an, welches ein auf wenige Meter genaues Lokalisieren der eigenen Position bzw. der von Freunden erlaubt und bereits mehr als zehn Millionen Nutzer in Japan hat [Lan05a].

[34] www.jackmobile.de

USA finden sich vermehrt ortsbasierte Dienstleistungen, seit der Gesetzgeber die genaue Lokalisierung von Mobiltelefonen bei Notrufen in der sogenannten *E-911*-Gesetzgebung vorgeschrieben hat.[35] So bieten Verizon mit *Chaperone*[36] und Sprint mit *Family Locator*[37] die Möglichkeit, das Handy der Kinder jederzeit auf einer Karte im Web bzw. auf dem eigenen Mobiltelefon zu lokalisieren, deren Bewegungen aufzuzeichnen oder auch – per SMS – einen zeit- und ortsabhängigen Alarm auszulösen (wenn beispielsweise der Sohn nicht rechtzeitig in der Schule eintrifft) [Yua06]. Auch Pionier Wherify hat bereits ein spezielles Kinder-Handy auf dem Markt, welches unabhängig vom Mobilfunkbetreiber funktioniert und zusätzlich spezielle Notfallknöpfe für die Kinder bereitstellt.[38] Zwar haben alle Systeme noch mit der Genauigkeit zu kämpfen [Bai06], doch mag die Kombination aus günstigem Preis (da die dazu nötige Infrastruktur durch *E-911* sowieso geschaffen werden muss) und einfacher Bereitstellung (da selbst die jüngsten Familienmitglieder wie selbstverständlich ein Mobiltelefon nutzen) für diese Art der Anwendung in naher Zukunft den Durchbruch bedeuten.

Man mag solchen Entwicklungen mit Argwohn begegnen und Eltern, die so ihr Kind „behüten", herzlos finden oder als Kontrollfanatiker abtun. Doch ist die Nachfrage nach derlei Überwachungstechnologie womöglich auch eine direkte Folge der gestiegenen Komplexität des täglichen Lebens, wie sie nicht nur gestresste Manager, hochflexible Dauerpraktikanten [Spi06b] oder eben berufstätige Eltern zu bewältigen haben. Den Trends zu mehr Flexibilität und Mobilität im Alltag scheinen „Lifestyle"-Produkte wie Mobiltelefon, e-Banking, 24h-Shopping und Navigationssystem fast schon zwingend zu folgen. Wenn das Mobiltelefon bald schon nicht nur die Ortung von Freunden und Familienangehörigen, sondern – etwa für einen geringen Monatsbeitrag – auch das Auffinden beliebiger persönlicher Gegenstände ermöglichen sollte [FRNS+06], würden womöglich viele Kunden bereitwillig den Aufenthaltsort ihrer Haus-, Büro- und Autoschlüssel überwachen lassen.

Ebenso populär könnten Gesundheits- und Freizeitanwendungen werden, die Konsumenten dabei helfen, eine ausgewogene Ernährung (bzw. Diätprogramme), ausreichend Bewegung, Arbeitspausen oder sportliche Trainingsprogramme im Alltag umzusetzen. Die US-amerikanische Firma BodyMedia[39] vertreibt bereits seit einigen Jahren mit Sensoren und Funkmodulen ausgestattete Armbänder, die

[35] Die sogenannte zweite Phase (*Phase II*) des *Enhanced 911*-Programms verlangt von Mobilfunkbetreibern, bei Notrufen (d.h. bei Anrufen auf 9-1-1) das Mobiltelefon bis auf 100 Yards genau (knapp über 90 Meter) orten zu können. Während einige Anbieter diese Lokalisierung via Triangulation durch die Basisstationen zu erzielen versuchen, setzen andere auf die Integration spezieller Ortungssysteme (z.B. GPS) in Mobiltelefone.

[36] www.verizonwireless.com/chaperone

[37] sfl.sprintpcs.com/finder-sprint-family

[38] Wherify's „Wherifone" hat inzwischen die firmeneigene Kinderuhr als Instrument der Wahl abgelöst, da diese zum Preis von knapp 400 Dollar offenbar nur schwer verkäuflich war (das Wherifone kostet unter 100 Dollar, kann aber im Gegensatz zur verriegelbaren Armbanduhr liegen gelassen werden) [All06].

[39] www.bodymedia.com

Kalorienverbrauch, Bewegung und sogar Schlafphasen messen und so Sportlern, ernährungsbewussten Verbrauchern bzw. deren Betreuern auf einer persönlichen Homepage detaillierte Angaben zum Ernährungs- bzw. Bewegungsprogramm machen können.[40] Das Wearable-Computing-Labor der ETH Zürich entwickelt einen in einer Gürtelschnalle verborgenen Computer, der drahtlos mit verschiedensten Sensoren verbunden werden kann, um detaillierte medizinische Daten oder auch Bewegungsmuster aufzuzeichnen und auszuwerten [ALOM+04].[41]

Nicht zuletzt treibt natürlich auch die Kommunikationstechnologie den Trend zur Digitalisierung unseres Lebens voran. Flexiblere Lebens- und Arbeitsmodelle, bei denen die Kinderbetreuung immer weniger alleinige Aufgabe der Mutter ist, und die mit der steigenden Globalisierung und Mobilität der Gesellschaft einhergehende berufliche Flexibilität erlauben es Firmen wie dem Webcam-Hersteller Axis[42], ihre Produkte nicht nur Sicherheitsfirmen zu verkaufen, sondern auch Müttern und Vätern, die während ihrer Geschäftsreise oder auch vom Büro aus kurz mal daheim „reinschauen" wollen, oder Großeltern, Kindern und Enkeln, um mit entfernt lebenden Verwandten in Kontakt zu bleiben. Die bei solchen Kameras oft unzureichend voreingestellten Sicherheitsparameter ermöglichen es inzwischen einer internationalen Besuchergemeinde im Internet, mit Hilfe clever formulierter Suchanfragen in fremde Wohn- und Schlafzimmer, Büros, Geschäfte oder Restaurants zu spähen, in den meisten Fällen wohl ohne Wissen – geschweige denn Einwilligung – der im Internet zu betrachtenden Personen [Spi06a].[43]

All dies sind Beispiele, wie detaillierte digitale Überwachungssysteme gezielt Kundenbedürfnisse erfüllen können, statt dass sie von skrupellosen Geschäftemachern gegen den Willen der Konsumenten erzwungen werden. Convenience-Produkte, die im komplexen modernen Alltagsleben das Organisieren erleichtern bzw. Zeit sparen, die uns in kleineren und größeren Notsituationen unterstützen (medizinische Überwachung, Notrufe, aber auch das Auffinden verlorener Gegenstände), oder die die globale Kommunikation mit Kollegen, Freunden und unserer Familie ermöglichen, werden in den meisten Fällen kaum als Einschränkung der Privatsphäre angesehen werden. Überhaupt ist fraglich, welchen Wert der Einzelne wirklich der eigenen Privatsphäre beimisst,[44] bzw. welche Informationen im Alltag schlussendlich dazu zählen [HaS01].

---

[40] Aus „technischen Gründen" erfolgt die Auswertung der aufgezeichneten Daten auf den zentralen Servern der Firma BodyMedia, die dadurch in den Besitz umfangreicher medizinischer Informationen ihrer Kunden kommt.

[41] Siehe auch den Beitrag von Tröster [Trö07] in diesem Band.

[42] www.axis.com/de

[43] Siehe auch die Webseiten johnbokma.com/mexit/2005/01/09/security-webcam-hunting.html, www.pixeljunkie.de/2006/02/06/google-webcam-hack oder www.opentopia.com/hiddencam.php.

[44] So musste die 1997 gegründete kanadische Start-up-Firma *Zero-Knowledge* ihr von Presse und Experten gleichermaßen gepriesenes Anonymisierungssystem *Freedom-Network* Ende 2004 vom Markt nehmen, da nicht genügend Kunden bereit waren, für anonymes Internetsurfen und nicht verfolgbares Versenden von E-Mail zu bezahlen [Sla04].

Während Industrie und Handel also die technische Entwicklung vorantreiben und die Basis für eine industrielle Massenproduktion ubiquitärer Systeme legen, damit also die *technische und ökonomische Grundlage* für deren Verbreitung bereitstellen, so dürften die um diese Technologien herum angebotenen individuellen Dienstleistungen und Produkte die *persönliche Akzeptanz* in der Bevölkerung erhöhen, sowie deren *Verbreitung im Alltag* vorantreiben, also die vielbeschworene „Durchdringung" unseres Lebens. Denn je mehr solcher Services vorhanden sind, desto leichter wird auch die Bereitstellung neuer Dienste vonstatten gehen, da diese womöglich bereits existierende digitale Daten in sogenannten *Mash-Ups*[45] für andere Zwecke wiederverwenden könnten – ein ubiquitärer Netzwerkeffekt.

Eine Zukunft voller neuer, datenhungriger Dienste also, die Dank der in Handel und Industrie vorangetriebenen ubiquitären Technologien immer günstiger und verlässlicher werden. Aber reicht dies, um die viel beschworene „totale Überwachung" unseres Lebens zu erreichen [AlM05]? Oder wird die Vielzahl an Anwendungen auf ähnlich vielen Datenbanken verteilt zwar einen quantitativen, aber kaum einen qualitativen Unterschied zu unserer heutigen Situation bedeuten? Die Idee, mit einer einfachen (und praktisch kostenlosen!) Internetsuche innerhalb weniger Sekunden „Briefe" (d.h. elektronische Nachrichten), Fotos oder gar Bewerbungsschreiben einer beinah beliebigen Person finden zu können, mag noch vor 50 Jahren unheimlich und gefährlich angemutet haben – heute würde wohl kaum einer auf die Idee kommen, deshalb die Abschaffung des Internets oder wenigstens der Suchmaschinenbetreiber zu fordern. Statt dessen hilft heute ein immer größer werdender Anteil der Bevölkerung (vor allem Kinder und Jugendliche) sogar noch aktiv dabei mit, auf „sozialen" Plattformen wie OpenBC/Xing, MySpace oder Flickr[46] ihre persönlichen Daten zu digitalisieren und weltweit verfügbar zu machen: Lebensläufe, Vorlieben und Interessen, Freundeskreise und Beziehungen, Urlaubsfotos und -filme. Doch nur wenige würden ihr heutiges Leben bereits einer orwellschen Überwachung ausgesetzt sehen. Wird sich diese Entwicklung einfach fortsetzen und unser Leben zwar immer mehr digitalisieren, sich qualitativ (also bezüglich der *gefühlten* Privatsphäre) jedoch kaum von unserer heutigen Situation unterscheiden?

Sicherheit und gesellschaftliche Kontrolle

Ein letzter Trend mag hier entscheidenden Einfluss nehmen: die Bestrebung, unser Leben sicher und fair zu gestalten. „Sicher" im Sinne des Schutzes vor Kriminalität und Terrorismus, aber auch im Sinne eines Schutzes vor der eigenen Nachlässigkeit. „Fair" im Sinne einer vom Verursacherprinzip geleiteten Gesellschafts-

[45] Der ursprünglich aus der Musikbranche stammende Begriff wird im Zuge der Web-Renaissance (auch *Web 2.0* genannt) für das Verknüpfen verschiedener Web-Dienste zu einem neuen Mehrwertdienst verwendet.

[46] Siehe www.openbc.com, www.xing.com, www.myspace.com bzw. www.flickr.com.

ordnung, in der jeder für seine Handlungen verantwortlich ist und für eigene Fehler zur Verantwortung gezogen wird, statt soziale und ökonomische Kosten auf die Mitbürger abwälzen zu können. Die fortschreitende Digitalisierung unserer Leben durch RFID, Miniatursensoren und eingebettete, ubiquitäre Rechner- und Kommunikationssysteme wird neue Möglichkeiten schaffen, diese Ziele besser denn je zu überprüfen und auch durchsetzen zu können. So findet sich nach Bereitstellung (durch das Streben nach wirtschaftlicher Effizienz) und Verbreitung der Technik (durch das Streben nach persönlicher Bequemlichkeit) schließlich auch der Imperativ zur umfassenden Nutzung der Daten durch unser Streben nach Gerechtigkeit und Sicherheit.

Prominentestes Beispiel ist sicherlich die weltweite Entwicklung nach den Anschlägen vom 11. September 2001. Es lässt sich heute kaum ein Land finden, in dem die staatlichen Kontroll- und Überwachungsmöglichkeiten seitdem nicht substantiell ausgedehnt wurden. Bekanntestes Beispiel ist wohl der im Oktober 2001 kurz nach den Anschlägen verabschiedete *USA-PATRIOT Act*[47], welcher den US-amerikanischen Strafverfolgungsbehörden weitreichende Zugeständnisse bei der elektronischen Überwachung machte [SoR03].[48] Auch in Europa wurden nach den Anschlägen vom März 2003 in Madrid und Juli 2005 in London verschärfte Gesetze erlassen, auf EU-Ebene vor allem die Telekommunikations-Direktive 2002/58/EC[49], die es nationalen Gesetzgebern freistellte, detaillierte Verbindungsdaten von Telefon- und Internetanbietern speichern zu lassen, und schließlich im Dezember 2005 die „Data Retention"-Direktive 2006/24/EC[50], welche die 2002er-Direktive novelliert und allen Kommunikationsanbietern eine Mindestspeicherdauer sämtlicher Verbindungsdaten von 6 Monaten vorschreibt [BBC05].

Ein Großteil der seit 2001 gesetzlich neu eingeführten Datensammlungen betrifft dabei Grenzkontrollen. Sichtbarstes Beispiel sind die neuen biometrischen Reisepässe, in denen ein drahtlos auslesbarer Funkchip zusätzlich zu den regulären Passdaten zunächst das Passbild digital zur Verfügung stellt, bald aber auch zwei Fingerabdrücke mit einschließen soll [Küg05]. Bereits seit 2004 werden im Rahmen des US-VISIT-Programms[51] alle Besucher der USA erkennungsdienstlich behandelt, d.h. Fingerabdruck und Lichtbild werden bei der Einreise aufgenommen, gespeichert und mit Listen gesuchter Terroristen verglichen. Weiterhin sollen massive Data-Mining-Projekte helfen, selbst noch unbekannte Terroristen aufzuspüren. So sollte das auf einem einfachen Namensvergleich zwischen Flugtickets und Fahndungslisten basierende Erkennungssystem CAPPS[52] in Zukunft

[47] Die Abkürzung steht für *„Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism"*.

[48] Das zunächst nur für fünf Jahre geltende Gesetze wurde im März 2006 mit klarer Mehrheit in Senat und Repräsentantenhaus für weitere vier Jahre beschlossen (H.R.3199 *„USA PATRIOT Improvement and Reauthorization Act of 2005"* und S.2271 *„USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006"*) [CNN06].

[49] eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

[50] eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT

[51] Eine Abkürzung für *„United States Visitor and Immigrant Status Indicator Technology"*.

[52] Die Abkürzung steht für *„Computer Assisted Passenger Prescreening System"*.

als CAPPS II bereits beim Kauf eines Flugtickets sämtliche verfügbaren staatlichen und kommerziellen Informationen über den Käufer auswerten (z.B. dessen letzte Flugreisen, Wohnorte, Arbeitgeber, Finanztransaktionen und Kreditkarteneinkäufe) und ihm einen von drei Risikocodes (grün, gelb, rot) zuweisen.[53] Ein noch umfassenderes nationales Programm wurde bereits mehrere Male aufgrund massiver öffentlicher Kritik eingestellt, nur um wenige Monate später unter anderem Namen neu aufgesetzt zu werden.[54]

Allen Initiativen gemeinsam scheint der Drang, möglichst alles Erfassbare auch tatsächlich erfassen (und auswerten) zu wollen – solange es nur irgendwie technisch und ökonomisch machbar erscheint.[55] Dabei erfreuen sich die staatlichen Datensammler durchaus einer substantiellen Unterstützung in der Bevölkerung. So gaben bei einer Umfrage unter 22 US-amerikanischen Firmen in der Touristik-Branche (Fluglinien, Autovermieter, Hotels und Reisebüros) wenige Monate nach den Anschlägen mehr als die Hälfte zu, bereits detaillierte Kundendaten freiwillig an Regierungsbehörden weitergegeben zu haben [Baa02].[56] Eine Umfrage unter mehr als 600 US-amerikanischen Bürgern kurz nach den Anschlägen im November 2001 fand 70-80% Zustimmung für die Ausweitung staatlicher Überwachungsvollmachten, z.B. zum Abhören von Telefongesprächen, Überwachung des Internetverkehrs, der Kreditkarten- und Steuerabrechnungen, Bankkonten, ja sogar von Schulakten [NKK01]. Umfrageexperten der Harvard University zeigten sich nicht überrascht: *„While civil liberties have broad public support, the public will support substantial limits on those freedoms when there are serious threats, either at home or from overseas"* [Les02].

Bestes Beispiel ist die Akzeptanz flächendeckender Videoüberwachung in Großbritannien. In keinem anderen Land der Erde sind so viele Überwachungskameras in Betrieb – Schätzungen aus dem Jahr 2004 gingen bereits damals von über vier Millionen Kameras aus.[57] Auch wenn die umfangreiche Forschung zum Nutzen der Videoüberwachung zu sehr gemischten Ergebnissen kommt [Joh06a, McN02], scheint in Großbritannien die Zustimmung zum Einsatz von Kameras

[53] Wegen massiver Kritik wurde die Arbeit an CAPPS II inzwischen offiziell eingestellt; das Nachfolgeprojekt *Secure Flight* verfolgt jedoch ähnliche Ziele.

[54] Das als *Total Information Awareness* (TIA) gestartete Programm wurde zunächst in *Terrorist Information Awareness* umbenannt, dann in *Novel Intelligence from Massive Data* (NIMD) und wird inzwischen unter dem Namen *Multistate Anti-Terrorism Information Exchange* (MATRIX) fortgeführt.

[55] Die US-amerikanische Raumfahrtbehörde NASA schlug sogar das Scannen von Gehirnwellen am Gate (mittels *„non-invasive neuro-electric sensors"*) vor, um „verdächtige Gedanken" oder Nervosität unter den Passagieren aufzuspüren [Let04].

[56] Selbst die mittels Kundenkarten erfassten Supermarkteinkäufe der Terroristen vom 11. September wurden bereits ausgewertet und förderten ein erstaunliches Profil potenzieller Terroristen zutage: *„One of the factors was if you were a person who frequently ordered pizza and paid with a credit card"* [Baa02].

[57] Schätzungen von Prof. Clive Norris, dem stellvertretenden Direktor des *Centre for Criminological Research* in Sheffield, anlässlich einer Konferenz im Januar 2004, basierend auf dessen Studie über die Verbreitung von Sicherheitskameras in London aus dem Jahr 2002 [McN02] (zitiert in [Mac04]).

ungebrochen, womöglich aufgrund einiger weniger spektakulärer Fahndungserfolge, wie etwa die Überführung zweier minderjähriger Mörder im Fall James Bulger 1993 in England [Zur04]. In bester Big-Brother-Manier bieten einige britische Kommunen inzwischen die Einspeisung der Überwachungskameras als sogenanntes „ASBO-TV“ [58] direkt ins Fernsehkabel an, komplett mit einblendbarer Fahndungsliste und anonym nutzbarer E-Mail-Meldeadresse [Swi06].[59] Selbst in Deutschland, wo die Bevölkerung traditionell der Videoüberwachung eher skeptisch gegenübersteht,[60] gab es so z.B. im Vorfeld der Fußball-Weltmeisterschaft 2006 eine knapp 85%-ige Zustimmung zu einer verstärkten Videoüberwachung öffentlicher Plätze [Spi06c], eine Studie des Instituts für Kriminologische Sozialforschung der Universität Hamburg fand eine ähnlich hohe Zustimmung in der Bevölkerung [Küp06]. Nach den schnellen Fahndungserfolgen im Zusammenhang mit den versuchten Anschlägen auf Nahverkehrszüge im Juli 2006 befürworten 80% der Deutschen eine weitere Ausweitung der Videoüberwachung auf Busse und Bahnen [Spi06d].

Während die heutige Videoüberwachung zwar abschreckend wirken kann (indem sie bei der Aufklärung hilft), doch wirkliche Verbrechen kaum zu verhindern weiß [Zur04], sollen nach Wunsch der Experten zukünftige Systeme aktiv das Geschehen beobachten können und in Gefahrensituationen rechtzeitig Alarm schlagen. Intelligente Programme sollen dabei helfen, in der zunehmenden Bilderflut automatisch verdächtige Personen und Verhaltensweisen erkennen zu können [Sch06b]. Auch wenn aktuelle Systeme noch kaum mit der Komplexität einfacher Alltagssituationen (z.B. wartende Reisende auf einem Bahnsteig) zurechtkommen, so versprechen neuere Detektionsalgorithmen wie Gesichts- oder Autokennzeichenerkennung bereits in naher Zukunft einen ersten Vorgeschmack auf solch eine automatisierte Überwachung. In der Stadt Zürich ist seit 2003[61] eine Pilotanlage des schweizerischen AFNES (Automatisches Fahrzeugnummernerkennungssystem) in Betrieb, welches die Kennzeichen aller stadteinwärts fahrenden Fahrzeuge mit der Fahndungsdatenbank des Bundes abgleicht und gestohlene Fahrzeuge bzw. solche ohne Versicherungsschutz innerhalb von Sekunden erkennt und die Zürcher Stadtpolizei alarmiert [StZ06]. Während das schweizer System bisher noch nicht flächendeckend ausgebaut wurde, ist dessen britisches Pendant, das *Automatic Number Plate Recognition System* (ANPR), seit Juni 2006 auf Londons

[58] Der Name rührt von dem in Großbritannien verbreiteten *„anti-social behavior order (ASBO)“* her, einem im Schnellverfahren von Streifenpolizisten aussprechbaren Verweis, der etwa Kiffern Zutritt zu einem Park oder 13-jährigen das Rauchen bis zur Volljährigkeit verbieten kann. Ein beispielsweise im ASBO-TV beobachteter Verstoß gegen diese Auflagen kann für die Betroffenen bis zu fünf Jahre Gefängnis bedeuten [Her06].

[59] In der nördlich von London gelegenen Stadt Peterborough werden seit Oktober 2006 sogar Passanten, die ihren Müll achtlos auf die Straße werfen, mit den von Überwachungskameras aufgezeichneten Bildern im Internet öffentlich zur Fahndung ausgeschrieben (siehe www.peterborough.gov.uk/page-9191).

[60] Noch 1998 wurde Deutschland als „Entwicklungsland“ in Bezug auf den Einsatz von Videoüberwachung bezeichnet [HeT02].

[61] Testläufe des seit 1996 entwickelten Systems fanden bereits im Jahr 2000 statt [Gro00].

gesamter Ringautobahn, der M25, in Betrieb. Auch hier können vorbeifahrende Fahrzeuge mit nationalen Fahndungssystemen verglichen werden, doch wird im Gegensatz zu AFNES, welches außer statistischen Informationen (Anzahl Fahrzeuge, Anzahl Alarme) keinerlei Daten speichert, die Bewegung aller erfassten Fahrzeuge für zwei Jahre gespeichert (bald sollen es fünf sein). Durch die Ausdehnung des Systems auf alle britischen Nationalstraßen erhofft man sich, gezielt nach Fahrzeugen suchen zu können, die sich zur Tatzeit im Umkreis eines Tatorts aufhielten [Jor06].[62] Ähnliche Pläne gibt es auch in Deutschland, wo neben ersten kamerabasierten Testsystemen in Niedersachsen [NIS05], Hessen und Bayern [Spi02] auch die Verwendung der zur Mautabrechnung erhobenen Daten zur Fahndung gesuchter LKW zur Diskussion steht [Bor05].

Besonders relevant an dieser Entwicklung ist vor allem der Umstand, dass ursprünglich für einen bestimmten Zweck erhobene Daten (z.B. zur Abrechnung der Londoner *City Charge* fotografierte Fahrzeuge) inzwischen wie selbstverständlich für weitere Zwecke (eben den Betrieb des ANPR-Systems) eingesetzt werden. Der Datenschutzexperte Gus Hosein von der London School of Economics nennt dies die „Entkriminalisierung des Datensammelns" [Hos06]: Während klassische Datenschutzgesetze wie etwa die EU-Direktive 95/46/EC[63] noch vom Grundsatz der Datensparsamkeit ausgingen, der Datensammlern vorschrieb, nur das Nötigste an Informationen zu erheben und diese Daten nach Zweckerfüllung umgehend zu löschen, macht Hosein in der aktuellen internationalen Gesetzgebung einen Drang zur ausgeprägten Vorratssammlung und späteren Sekundärnutzung (*re-purposing*) ausfindig. Als Beispiel zitiert er den Aufbau der nationalen Gendatenbank in Großbritannien, die anfangs lediglich die genetischen Daten verurteilter Sexualstraftäter enthalten sollte, inzwischen aber schrittweise ausgeweitet wurde – zunächst auf andere Straftaten (Gewaltverbrechen, später Kapitalverbrechen), dann auf lediglich angeklagte (aber noch nicht verurteilte) Personen, später auf nur schon unter Verdacht stehende Straftäter. Seit 2001 können grundsätzlich genetische Fingerabdrücke *aller* lediglich unter Verdacht stehenden Personen in der Datenbank gespeichert werden – weder ist eine Anklage noch eine Verurteilung nötig. Im November 2004 bestätigte das nationale britische Berufungsgericht (der Court of Appeal) die Rechtmäßigkeit dieses Verfahrens: *„It is of paramount importance that law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science… It is in the public interest in its fight against crime for the police to have as large a database as possible... The more complete the database, the better chance of detecting criminals, both those guilty of crimes past and those whose crimes are yet to be committed. The better chance too of deterring from future crime those whose profiles are already on the database"* [StW04]. „Wer ehrlich ist, hat nichts zu verbergen" lautet die Formel, deren wundersame Implikationen ein Teilnehmer eines rechtswissenschaftlichen Diskussionsforums[64] so beschreibt: *„Wer gegen*

[62] John Dean, der nationale Koordinator des APNR-Projekts, umreißt das Ziel des Systems so: *„Our aim is to deny criminals the use of the roads"* [Jor06].

[63] eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

[64] www.lawblog.de/index.php/archives/2005/10/27/drei-worte/

eine DNA-Datenbank ist oder sich gegen einen Eintrag in eine solche DNA-Datenbank ausspricht, der muss m.E. irgendwie ‚Dreck am Stecken' haben. Bei einer Aufnahme in eine DNA-Datenbank entsteht niemanden ein Schaden und weh tuts auch nicht. Wäre ganz Deutschland in einer großen DNA-Datenbank erfasst, gäbe es keine Kriminellen mehr: Alle gehen in die Arbeit, es gibt keine 5 Millionen Arbeitslosen mehr. Auch die Schwarzarbeit ist ein Fremdwort."[65]

Inzwischen befinden sich über 3,6 Millionen Einträge in der britischen Gendatenbank [Joh06b, Wik06b], über 25 000 davon von Minderjährigen [Joh06a]. Wie schnell auch Kinder-DNA in die Täterdatenbank gelangt, zeigt ein Beispiel vom Juli 2006: Polizisten nahmen nordwestlich von London drei 12-jährige Kinder fest, die in einem Baum in einem öffentlichen Park spielten. Die Kinder wurden mit auf die Wache genommen, mussten ihre Schuhe ausziehen, wurden erkennungsdienstlich behandelt (d.h. sie wurden fotografiert und es wurde eine Speichelprobe für eine DNA-Analyse entnommen) und für zwei Stunden in eine Zelle gesperrt. Ein Polizeisprecher verteidigte die Vorgehensweise: *„West Midlands Police deals robustly with anti-social behaviour. By targeting what may seem relatively low-level crime we aim to prevent it developing into more serious matters"* [Sac06].[66]

Das Beispiel der britischen Gendatenbank illustriert anschaulich die Gefahr der weltweit vorangetriebenen Datensammlungen: Sobald einmal Daten erfasst wurden, wird es schwer, diese wieder zu löschen – sie könnten sich ja in Zukunft als nützlich erweisen (und wer will schon dafür verantwortlich sein, auf diese Art beispielsweise ein Verbrechen begünstigt zu haben). Einer ähnlichen Logik folgt die Debatte um die Haftentlassung von Sexualstraftätern. So müssen sich in den USA gemäß bundesstaatlicher Gesetze, die als *Megan's Law* bekannt geworden sind, entlassene Sexualstraftäter je nach Bundesstaat beim Einzug in eine Wohnung bei der lokalen Polizeistation anmelden, auf einer öffentlichen Webseite ihre neue Adresse eintragen, bzw. ein Schild im Vorgarten oder einen Aufkleber auf dem Auto anbringen mit den Worten „Hier wohnt/fährt ein registrierter Sexualstraftäter" [SoR03].[67] In Florida zwingt der *Jessica Lunsford Act* seit 2005 alle

[65] Schon vor hundert Jahren sah man sich so dank des Segens der Technik (der drahtlosen Kommunikation in diesem Fall) bereits an der Schwelle zu einer verbrechensfreien Gesellschaft: *„Das drahtlose Jahrhundert wird also sehr vielen Verbrechen ein Ende machen. Es wird ein Jahrhundert der Moralität sein, denn bekanntlich sind Moralität und Furcht ein und dasselbe"* [Slo10].

[66] Inzwischen werden beispielsweise Informationen aus der britischen Gendatenbank auch für das Auffinden spuckender Jugendlicher verwendet [Edw05]. Ebenfalls ab 12 Jahren ist ein Eintrag in der schweizer Hooligan-Datenbank möglich – es genügen die bloße Nähe zu gewaltätigen Handlungen bzw. „Vermutungen" seitens eines Vereinsfunktionärs, man könne sich in Zukunft zu Gewalttaten hinreißen lassen, um für 10 Jahre gespeichert zu werden. Ein Eintrag kann auch für Nicht-Fußballfans ernste Folgen haben: So wurden beispielsweise zur Fußball-Weltmeisterschaft 2006 Personen, deren Name auf einer europäischen Hooligan-Liste zu finden war, für die Dauer der Wettkämpfe mit Ausreiseverboten belegt [NZZ06].

[67] Dabei ist anzumerken, dass in vielen US-Bundestaaten auch homosexuelle Handlungen oder oraler Sex als Sexualstraftat gelten, oder etwa der einverständliche Geschlechtsver-

wegen sexuellen Kindesmissbrauchs Verurteile zum lebenslangen Tragen einer GPS-Fußfessel [Röt05], in Kalifornien stimmten im November 2006 mehr als 70 Prozent der Wähler für den *Sexual Predator Punishment and Control Act: Jessica's Law*, welcher das lebenslange Tragen von GPS-Sendern für *alle* Sexualstraftäter zur Pflicht machen soll [Röt06].[68] Bereits 2004 sprach sich die schweizer Bevölkerung in einer Volksabstimmung für eine lebenslange Verwahrung sogenannter nicht-therapierbarer Sexualstraftäter aus. Ein psychologisches Gutachten muss dabei bereits bei der Verurteilung dem Angeklagten attestieren, dass in der Haft Aussicht auf Heilung besteht und er nach dem Absitzen der Haftstrafe dereinst wieder ohne Gefahr in die Gesellschaft entlassen werden kann. Will kein Gutachter eine solche Garantie abgeben, bleibt der Täter auch nach Beendigung seiner Haftstrafe in lebenslanger „Verwahrung" [BSE03].[69]

Die persönliche Sicherheit muss allerdings nicht immer nur von anderen – Terroristen, Mördern oder Sexualstraftätern – bedroht werden. In vielen Fällen bringen sich Bürger sogar selbst in Gefahr, wenn sie beispielsweise ohne Sicherheitsgurt Auto fahren oder sich ungesund ernähren. Auch hier liegt es mehr und mehr im Trend, staatliche Schutzmaßnahmen zu ergreifen. Sogenannte *paternalistische* Staaten zwingen ihre Bürger zur Teilnahme an staatlichen Kranken-, Renten-, oder Arbeitslosenversicherungen; sie schreiben Motorradfahrern Helme vor oder verbieten das Baden ohne die Anwesenheit eines Bademeisters [Dwo05]. Neben diesem „harten" Paternalismus setzen Regierungen in den letzten Jahren verstärkt auf „sanfte" Varianten (*soft paternalism* [Eco06]), die keine gesetzlichen Zwänge schaffen, sondern durch andere Anreize (z.B. finanzielle) versuchen, das Verhalten des Einzelnen zu beeinflussen. So wurde beispielsweise erst kürzlich in Großbritannien der bereits seit den 1980er-Jahren kursierende Vorschlag einer „Fett-Steuer" für Fast Food, Süßwaren und Softdrinks wieder ins Gespräch gebracht [BBC04, Cor06c].[70]

Andere oft diskutierte Beispiele für einen „sanften" Paternalismus sind etwa die Krankenkassen- oder Unfallversicherungsprämien, die den individuellen Lebensstil des Versicherten berücksichtigen: Wer nicht raucht, sich gesund ernährt oder viel bewegt sollte eine niedrigere Krankenkassenprämie zahlen, wer eine Risikosportart wie Bergsteigen oder Fallschirmspringen betreibt, eine höhere Unfallversicherung. In einer Umfrage des schweizerischen Krankenkassenverbandes Santésuisse sprachen sich im Jahr 2006 über 65% der Befragten für ein solches Modell aus [Cor06a]. Ähnlich positiv bewertet wird etwa die Idee, Autoversicherungsprämien nach dem individuellen Fahrstil zu berechnen [Cor06b]: Wird etwa abrupt beschleunigt oder abgebremst bzw. bei Nacht oder Regen gefahren, so ist die Prämie höher, als wenn man gemächlich bei Trockenheit und Sonnenschein

kehr eines 16-jährigen mit einer 15-jährigen (Tatbestand: Unzucht mit einer Minderjährigen) [SoR03].

[68] Beide Gesetze sind nach Kindern benannt, die in dem jeweiligen Staat bei einem Sexualverbrechen starben.

[69] Eine Ausnahme besteht lediglich, wenn „neue wissenschaftliche Erkenntnisse" eine mögliche Heilung des Täters in Aussicht stellen.

[70] Siehe auch den Beitrag von Spiekermann und Pallas [SpP07] in diesem Band.

außerhalb der Hauptverkehrszeiten fährt – eine Monatsabrechnung summiert dann die individuellen Fahrten zu einer Gesamtprämie. Progressive, ein US-amerikanischer Versicherer, testete zwischen 1998 und 2000 ein kilometergestütztes System namens *Autograph*, welches zusätzlich die Tageszeit und Gegend der jeweiligen Fahrt berücksichtigte.[71] Norwich Union, ein britischer Autoversicherer, bietet seit 2005 Fahranfängern eine *„Pay-As-You-Drive"* Versicherung an, bei der die Versicherungssumme ebenfalls dynamisch der Fahrweise angepasst wird.[72] Presseberichten zufolge wurden beide Angebote von den Kunden äußerst positiv bewertet, konnten sie doch in den meisten Fällen ihre monatliche Versicherungsprämie um bis zu 25% senken [Fre00] (Norwich Union verspricht sogar bis zu 35% Einsparungen [Cic06]).

Neben den individuellen Einsparungen versprechen solche *„Pay-As-You-Live"*- bzw. *„Pay-As-You-Drive"*-Produkte auch für den Versicherer signifikante Gewinne, da dieser das individuelle Risiko eines Versicherungsnehmers auf diese Weise viel genauer einschätzen und dadurch den „guten Risiken" günstigere Prämien anbieten kann, während die „schlechten" für ihr hohes Risiko nun weitaus mehr bezahlen müssen.[73] Doch gerade auch für den Staat sind solche Angebote attraktiv, ermöglichen sie doch genau die Art von sanftem Paternalismus, der ganz ohne Zwang die Bürger zu sichereren Autofahrern bzw. gesünderen Menschen erziehen könnte und damit gezielt die oft millionenschweren Aufklärungsprogramme der Regierungen unterstützen würde. Und nicht zuletzt entspricht es mehr und mehr einem in der Bevölkerung vorherrschenden „Fairness"-Prinzip, welches die bis dato dominierende Solidargemeinschaft zu hinterfragen beginnt, in der die Gesunden und Vorsichtigen nicht mehr für den riskanten Lebensstil der Raucher, Alkoholiker, Fast-Food-Anhänger oder Risikosportler bezahlen wollen [Cor06a].

Durch den Einsatz ubiquitärer Sensor- und Kommunikationstechnologie wird sich also in Zukunft ein immer größerer Anteil unseres Lebens überwachen und damit „optimieren" lassen: Wie wir Auto fahren [Cor06b], wie viel wir uns bewegen [ALOM+04] oder was wir essen [ASLT05]. Die „allwissende" Technik könnte also nicht nur das Aufklären von Verbrechen ermöglichen[74] oder das Vermeiden von Unfällen erleichtern, sondern auch die finanziellen Lasten im Staat fairer verteilen und uns (ganz sanft und freiwillig) zu einem „besseren" Leben führen.

Schlussfolgerungen

Werden wir in Zukunft noch eine Privatsphäre haben? Werden wir auch im Zeitalter des *Ubiquitous Computings* ein weitgehend selbstbestimmtes Leben

[71] www.epa.gov/projectxl/progressive/index.htm
[72] www.norwichunion.com/pay-as-you-drive
[73] Andreas Schraft, Head Risk Engineer des schweizer Rückversicherers SwissRe, nennt diese *„risk communities of one"* (zitiert in [Cor06b]).
[74] Wenn nicht sogar, durch Abschreckung, Verbrechen verhindern.

führen können? Oder läuft die momentane technische Entwicklung unweigerlich darauf hinaus, dass drahtlose Miniatursensoren oder „intelligente" Autos uns jederzeit und überall überwachen und unsere Handlungen und Bewegungen für die Ewigkeit aufzeichnen? Werden vielleicht Wirtschaft, Bevölkerung und Regierung dieser Entwicklung ökonomische, soziale oder rechtliche Grenzen setzen, wenn schon technisch prinzipiell fast alles machbar erscheint?

Datenschutz und Privatsphäre lagen schon seit jeher im Spannungsfeld zwischen wirtschaftlicher Effizienz, persönlicher Bequemlichkeit und allgemeiner Sicherheit. Die in der Presse beschriebenen Szenarien einer allgegenwärtigen Überwachung stoßen zu Recht auf starke Ablehnung unter den Verbrauchern: *„Wie ist es: würde es Sie, liebe Zuschauer, stören, wenn in Ihrem Pass ein Funkchip versteckt wäre – darin alle möglichen privaten Daten gespeichert. Behörden oder Unternehmen könnten herausschnüffeln, wo Sie gerade sind, welche Automarke Sie gerade fahren, welche Krankheit Sie plagt und ob Sie Arbeitslosengeld beziehen"* [Zei04]. Bedenklich wäre sicherlich, wenn das kaum jemanden stören würde! Doch womöglich ist die Frage ganz einfach falsch gestellt [HaS01]: *„Wie ist es: würde es Sie, liebe Leser, stören, wenn in allen Pässen zukünftig ein Funkchip versteckt wäre – der Terroristen, Verbrecher und illegale Ausländer an der Grenze auffliegen lassen würde, Ihnen an jedem Ort der Erde den Weg weisen könnte und Ihnen bei Unfall oder Krankheit die bestmögliche Behandlung garantieren würde?"* Wäre das so unangenehm?

Fest steht: Noch nie gab es so viele gute Gründe, Daten über sich preiszugeben (und dafür einen guten Preis zu erzielen). Wie weit sind wir bereit, ein Gut handelbar zu machen – nämlich unsere persönlichen Daten –, die zuvor anscheinend kaum weniger oft gesammelt wurden, aber für die man nichts bekam? Eingekauft wurde auch früher schon, da wusste ja auch der Verkäufer im Laden um die Ecke, wie viele Flaschen Wein ich die Woche dort im Durchschnitt kaufe. Nicht, dass sich noch nie jemand für diese Informationen interessiert hätte – es war ganz einfach bisher viel zu aufwändig, diese Daten über uns mühsam in Erfahrung zu bringen. Doch im Zeitalter von RFID und Kundenkarte kann man nun fast überall und dauerhaft Geld sparen, einfach indem man Dinge, „die eh schon jeder weiß", gewinnbringend verkauft. Beispielsweise jetzt auch für den Ferienflug Meilen sammeln – da wäre man ja schön dumm, wenn man nicht einfach noch diese Flüge aufs Meilenkonto schreiben lässt – die Fluggesellschaft kennt mich und mein Reiseziel ja sowieso.[75]

Oder – wie konnte man früher eigentlich nur ohne Mobiltelefon leben? Wer hat denn noch Zeit, zur Bank oder bald schon zum Supermarkt zu gehen? Wie bequem, dass sich das alles inzwischen von überall aus in der Welt via Internet erledigen lässt! Welche Eltern würden sich nicht darüber freuen, wenn der entlaufene Fünfjährige nicht etwa raus auf die Strasse gerannt ist, sondern – seiner

[75] Die Schlussfolgerung *„die haben die Daten ja eh, da kann ich auch noch etwas davon profitieren"* ist natürlich falsch: Ohne Nutzung einer Vielflieger- oder Kundenkarte müssen etwaige personenbezogene Daten nach Erbringung des Serviceangebots gelöscht werden (bzw. neu laut Direktive 2006/24/EC erst nach 6-24 Monaten). Auch haben Studien gezeigt, dass Kundenkarten oft keine Einsparungen bringen [Van00].

smarten Armbanduhr sei Dank – sich hinter dem Gebüsch im Garten beim Versteckenspielen finden lässt? Und seit die Attentate von Madrid und London auch Europa als potenzielles Ziel fanatischer Terroristen etabliert haben – wer mag da schon die Arbeit der Ermittlungsbeamten behindern, nur um der Freundin anonym per Telefon sagen zu können, wann man sich am Abend treffen will? Wer sollte etwas dagegen haben, dass die DNA von (tatsächlichen und potenziellen) Straftätern in einer Datenbank gespeichert wird, um die Aufklärung von Verbrechen zu ermöglichen?

Sollten wir in Zukunft immer stärker von der Technik überwacht werden, so wird wohl kaum die staatliche Schikane als Triebfeder dieser Entwicklung wirken, da man annehmen darf, dass demokratische Gesellschaften eine willkürliche Einschränkung ihrer bürgerlichen Freiheiten nur schwer hinnehmen werden. Aus einem „guten" Grund allerdings – zur Wahrung der Sicherheit, Verbesserung der Gesundheit oder Erleichterung des Alltags etwa – mögen solche Einschnitte durchaus akzeptabel sein. Die wirtschaftliche Entwicklung wird, mehr oder weniger entkoppelt von dieser Diskussion, die Entwicklung und den Einsatz ubiquitärer Technologien in jedem Fall weiter vorantreiben. Die Möglichkeit, Produktion und Vertrieb in Echtzeit zu beobachten und dadurch auch zu steuern, wird Einsparpotenziale und neue Geschäftsmodelle hervorbringen. Kontrollmöglichkeiten bis ins Wohnzimmer des Konsumenten hinein werden den Verkauf immer günstigerer Produkte erlauben (von denen dem Käufer aber immer weniger gehört), die so neue Käuferschichten erschließen können. Auch hier werden Kunden kaum ohne Grund eine Überwachung in Kauf nehmen, sondern Angebote vergleichen und jene mit einem greifbaren Mehrwert bevorzugen. Der als Beispiel mehr als überstrapazierte „smarte Kühlschrank"[76] als letztes Glied einer lückenlosen Liefer- und Werbekette ist heute eher ein abschreckendes Beispiel einer technikverliebten und realitätsfernen Forschungs- und Marketingmaschine als realistisches Ziel einer mit ubiquitärer Technik ausgestatteten Zukunft.[77]

Vor diesem Hintergrund bleibt in jedem Fall fraglich, ob das klassische Kontrollparadigma des Datenschutzrechts in Zukunft noch praktikabel sein wird. Bisher galt dem Datenschutz größtenteils Genüge getan, wenn der Kunde auf die Datensammlung aufmerksam gemacht wurde und seine explizite Einwilligung

[76] Zahlreiche Kritiker des Ubiquitous Computing haben dieses Haushaltsgerät bereits der Lächerlichkeit preisgegeben, sogar ein Comic über „Frigomax – der Kühlschrank auf Draht" existiert (www.itoons.de/comics/frigomax).

[77] Unabhängig vom potenziellen Bedarf nach einem automatisch Milchtüten nachbestellenden Haushaltsgerät bleibt derzeit die verlässliche technische Umsetzung solch einer Vision fraglich. Auch IBMs Vision eines Supermarktes ohne Kassenschlangen (siehe beispielsweise www.youtube.com/watch?v=WPtn0fM4tuo bzw. die Suche nach „IBM" und „RFID" auf www.youtube.com) scheint in naher Zukunft kaum machbar: zu unzuverlässig lassen sich RFID-Etiketten aus einer Einkaufstasche heraus lesen, zu einfach ist ein „zufälliges" Abschirmen von Tags durch Alufolie möglich, als dass ein verlustfreies automatisches Abrechnen möglich wäre.

eingeholt wurde (z.B. durch die Unterschrift auf dem Kundenkartenantrag).[78] Weisers *„privacy is really a question of control"*-Ansatz folgt hier dem Ideal des verantwortungsvollen Benutzers, der sich jederzeit der Implikationen seiner Handlungen bewusst ist. Zwar sind offene Datensammlungen, die dem Datensubjekt die Partizipation weitgehend freistellen, sicherlich eine notwendige, bald aber vielleicht nicht mehr hinreichende Bedingung für einen wirkungsvollen Schutz unserer Privatsphäre. Es könnten in Zukunft einfach zu viele, zu unscheinbare Datenerhebungen sein, als dass der Einzelne das Für und Wider einer solchen Sammlung wirklich prüfen könnte.

Dabei wäre nicht nur die Frequenz solcher Entscheidungen angesichts hunderter smarter Dienste in Zukunft kaum praktikabel [Lan01],[79] vor allem bliebe fraglich, ob man sich über die Implikationen angesichts der Komplexität des jeweiligen Erhebungskontexts überhaupt im Klaren sein könnte. Wen sollte es schon interessieren, was ich heute Nachmittag für Lebensmittel einkaufe oder was für Musik ich auf dem Nachhauseweg im Auto höre? Eine Studie der Universität Leicester fand beispielsweise Zusammenhänge zwischen der bevorzugten Musikstilrichtung und sexuellen Neigungen (Hip-Hop und Dancemusic-Liebhaber wechseln oft ihre Sexualpartner, Countrymusic-Fans selten) oder Drogenkonsum (über 25% aller Opernfans haben schon einmal Haschisch probiert) [Lei06]. Und einem Supermarktkunden in Kalifornien wurde seine Kundenkarte zum Verhängnis, als er nach einem Unfall (er war auf einer Joghurtlache im Supermarkt ausgerutscht) den Besitzer auf Schadensersatz verklagen wollte: Der fand nämlich „überdurchschnittlich" viel Alkoholika im Einkaufsprofil des Kunden und drohte damit, bei einer Anklage den Geschworenen dies als Beweis für die womöglich wahre Unfallursache (Trunkenheit des Kunden) zu präsentieren [Vog98].

Fraglich bleibt auch, ob eine totale Überwachung unseres Lebens wirklich zu mehr Sicherheit und Gerechtigkeit führen wird, stellen diese Trends doch die wesentlichsten Einschränkungen unserer Freiheiten dar. Gerade die psychologischen Folgen einer vermeintlich „sicheren" Technik könnten signifikant sein, da einer vermeintlich „objektiven" Beurteilung einer Situation (oder einer Person) durch ein Computersystem schnell ein Hauch von Unfehlbarkeit anhaftet. Der Soziologe Gary T. Marx nennt dies *the fallacy of the 100% fail-safe system*: *„This involves the belief that machines do not make mistakes or cannot be fooled and issues of reliability and validity. The claim ‚but the computer says' or ‚it is in the computer' illustrates this fallacy, as if that offered religious or parental authority, or was equivalent to a law of nature. Even if it is ‚in' the computer that does not guarantee its accuracy, or appropriateness"* [Mar03]. Bestes Beispiel ist die

[78] Natürlich schreiben Datenschutzgesetze noch weitaus mehr vor, doch gelten die beiden Grundsätze von *Notice* und *Choice* – das Bekanntgeben einer Datensammlung und die explizite Wahlmöglichkeit des Datensubjekts – als Grundpfeiler des modernen Datenschutzes [MaL01].

[79] Studien zeigen, dass beispielsweise Internetnutzer in den meisten Fällen die Sicherheitswarnungen ihrer Browser-Software ignorieren und auf die Frage „Wollen Sie weitermachen?" grundsätzlich auf „Ja" klicken [ZKSB02].

Einführung des biometrischen Reisepasses, dessen integrierter RFID-Chip dank digitaler Signatur zwar fälschungssicher (d.h. nicht veränderbar) ist, nicht aber vor dem bloßen Kopieren geschützt ist.[80] Auch wenn hier rein technisch kaum von einem Versagen eines Sicherheitssystems gesprochen werden kann (die *ePass*-Spezifikation weist sogar explizit auf die Möglichkeit des Kopierens hin: *„Does not prevent an exact copy of chip AND conventional document"* [ICA04]), so warnen Experten davor, dass ein konventionell gefälschter Reisepass mit Hilfe eines kopierten RFID-Chips womöglich glaubhafter erscheinen könnte: *„Note also that the mere presence of the reader, the chip and the general ePassport security pixie dust will… have a psychological effect on border control staff. They will tend, because the machine says the passport is clean, to drop their guard, not really inspect either picture or bearer properly. This kind of effect is well documented, and it's the same kind of thing as people walking in and out of companies unchallenged despite wearing a security tag in the name of ‚Michael Mouse'"* [Let06].

Ebenso problematisch könnten die immer detaillierteren Sicherheitsprofile werden, die zwar das erklärte Ziel haben, „unschuldige" Personen von übermäßigen Sicherheitskontrollen zu befreien, dies aber zu Lasten der nun weniger, dafür aber umso verdächtiger gewordenen „nicht-so-klar Unschuldigen": *„[Air Travel Safety Programs] generate a whole new class of innocent but redlisted passengers who only fly when they're sufficiently desperate to face taking three days (or who knows, three years) to check in"* [Let04]. Bestes Beispiel ist US-Senator Edward „Ted" Kennedy, dessen Name im März 2004 auf die (inzwischen mehrere zehntausend Namen umfassende [Goo05]) „No-Fly"-Liste des US-amerikanischen *Department for Homeland Security* geraten war, da ein mutmaßlicher Terrorist den Decknamen „T. Kennedy" verwendet hatte [Goo04]. Nicht zuletzt zeigen die Beispiele der britischen Gendatenbank oder die Liste der US-amerikanischen Sexualstraftäter, wie schnell auch „kleine Fische" (Kinder, Teenager) ganz offiziell auf Listen landen können, die ursprünglich Schwerstverbrechern, Terroristen oder Triebtätern vorbehalten waren.[81]

Werden wir in einer informatisierten Welt noch eine Privatsphäre haben? Letztendlich liegt es an uns, welchen Wert wir dem Datenschutz in Zukunft beimessen werden. Mit Hilfe ubiquitärer Technik wird aller Voraussicht nach in naher Zukunft eine beinahe lückenlose Digitalisierung unseres Lebens möglich sein, die uns zwingen wird, unsere gesellschaftlichen Werte zu hinterfragen. Wie „perfekt" soll unsere Gesellschaft werden? Wie viel Abweichung verträgt sie? Warum nicht die totale Überwachung, um nie mehr einen Straftäter straffrei ausgehen zu lassen? Warum nicht „smarte" Autos, die keine Raser und Falschparker mehr entwischen lassen (oder womöglich Rasen und Falschparken erst gar nicht mehr mög-

[80] So wurde etwa ein in einem deutschen *ePass* integrierter Chip im Sommer 2006 an der alljährlichen „Black Hat"-Sicherheitskonferenz vor den Augen der Teilnehmer ausgelesen und auf eine handelsübliche Smartcard übertragen [Let06].

[81] So fanden sich beispielsweise auf der ursprünglichen Anti-Terrorliste von CAPPS I nicht nur Terroristen, sondern auch politische Aktivisten und Anti-Kriegsgegner [Röt03].

lich machen)? In einer demokratischen Gesellschaft werden wir diese Entscheidung bewusst treffen müssen, damit sie uns nicht durch die vorherrschenden Trends nach Effizienz, Bequemlichkeit und Sicherheit schleichend und unbemerkt aufgezwungen werden.

As nightfall does not come at once, neither does oppression.
It is in such twilight that we all must be aware of change in the air
– however slight – lest we become victims of the darkness.
William O. Douglas, Richter am obersten US-Bundesgericht, 1898-1980

Literatur

[AIM01] Association for Automatic Identification and Data Capture Technologies (AIM) (2001) Shrouds of Time – The History of RFID. www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

[All06] Alleven M (2006) Wherify Finds Way into Toys "R" Us. Wireless Week Website, 22. August 2006. www.wirelessweek.com/article/CA6364663.html

[AlM05] Albrecht K, McIntyre L (2005) Spychips: How Major Corporations and Governments Plan to Track Every Move with RFID. Nelson Current, Nashville

[ALOM+04] Amft O, Lauffer M, Ossevoort S, Macaluso F, Lukowicz P, Tröster G (2004) Design of the QBIC wearable computing platform. In: Cavallaro JR, Thiele L, Rajopadhye S, Noll TG (eds.) Proc. 15th IEEE Int. Conf. on Application-Specific Systems, Architectures and Processors (ASAP 2004), Sep. 27-29, 2004, Galveston, Texas.

[And03] Anderson R (2003) 'Trusted Computing' Frequently Asked Questions. Version 1.1, August 2003. www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[ASLT05] Amft O, Stäger M, Lukowicz P, Tröster G (2005) Analysis of chewing sounds for dietary monitoring. In: Beigl M, Intille S, Rekimoto J, Tokuda H (eds.) UbiComp 2005: Ubiquitous Computing. 7th International Conference, UbiComp 2005, Tokyo, Japan, September 11–14, 2005, Proceedings. Lecture Notes in Computer Science, vol 3660. Springer, Berlin Heidelberg New York, 56–72

[ASE05] Association européenne des concessionaires d'autoroutes et d'ouvrages à péage (2005) The Italian Motorway Network at 31. ASECAP Website. www.asecap.com/presentations-vienna-2005/national%20reports/9_Italy_E.pdf

[ASE06] Association européenne des concessionaires d'autoroutes et d'ouvrages à péage (2006) Italian Motorway System as of 31.12.2005. Konferenz-Website der *34th Study and Information Days of ASECAP*, Pula, Kroatien, 21.-24. Mai 2006. www.asecap2006.com.hr/national_r/ASECAP_Italijaeng.pdf

[Baa02] Baard E (2004) Buying trouble – your grocery list could spark a terror probe. The Village Voice, 30. Juli 2002. www.villagevoice.com/news/0230,baard,36760,2.html

[Bai06] Baig EC (2006) Where's Junior? The phone knows. USA Today, Cyberspeak, 21. April 2006. www.usatoday.com/tech/columnist/edwardbaig/2006-04-19-sprint-family-tracker_x.htm

[BBC02] BBC (2002) Police can keep suspects' DNA. BBC.com, 12. September 2002. news.bbc.co.uk/1/hi/uk/2254053.stm

[BBC04] BBC (2004) Government unit 'urges fat tax'. BBC.com, 19. Februar 2004. news.bbc.co.uk/2/hi/health/3502053.stm

[BBC05] BBC (2005) EU approves data retention rules. BBC.com, 14. Dezember 2005. news.bbc.co.uk/2/hi/europe/4527840.stm

[BCL04] Bohn J, Coroama V, Langheinrich M, Mattern F, Rohs M (2004) Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications. Human and Ecological Risk Assessment 10(5): 763–786

[BGSJ+05] Bono SC, Green M, Stubblefield A, Juels A, Rubin AD, Szydlo M (2005) Security Analysis of a Cryptographically-Enabled RFID Device. In: McDaniel P (ed.) Proc. 14th Usenix Security Symposium, July 31–August 5, Baltimore, MD, USA. USENIX Assoc., Berkeley, 1–16. www.usenix.org/events/sec05/tech/bono/bono.pdf

[Bis06] Bissantz N (2006) Mythos Data Mining. Bissantz & Company GmbH Website. www.bissantz.de/kolumne/mythos_data_mining

[Bor05] Borchers D (2005) LKW-Maut: Minister will offenbar Fahndung mit Mautdaten erlauben. Heise News, 26. November 2005. www.heise.de/newsticker/meldung/66676

[BSE03] Die Bundesversammlung der Schweizerischen Eidgenossenschaft (2003) Bundesbeschluss über die Volksinitiative „Lebenslange Verwahrung für nicht therapierbare, extrem gefährliche Sexual- und Gewaltstraftäter". www.admin.ch/ch/d/ff/2003/4434.pdf

[Bun05] Deutscher Bundestag (15. Wahlperiode) (2005) Antwort der Bundesregierung auf die Große Anfrage der Abgeordneten Gisela Piltz, Ernst Burgbacher, Rainer Funke, weiterer Abgeordneter und der Fraktion der FDP: Überprüfung der personengebundenen datenschutzrechtlichen Bestimmungen. Drucksache 15/4725. www.bundestag.de/aktuell/hib/2005/2005_037/01.html

[Cic06] Cicutti N (2006) Firms launch innovative pay-as-you-drive policies. Sunday Herald Website, 24. September 2006. www.sundayherald.com/58064

[CNN06] CNN (2006) House approves Patriot Act renewal. CNN.com, 7. März 2006. www.cnn.com/2006/POLITICS/03/07/patriot.act/

[Col06] Collins J (2006) RFID's Impact at Wal-Mart Greater Than Expected. RFID Journal Website. www.rfidjournal.com/article/articleview/2314/1/1/

[CoN06] Contactless News (2006) Successful trial leads to NFC deployment by Nokia, Philips, RMV, and Vodafone in Hanau, Germany. Contactless News Library Website, 19. April 2006. www.contactlessnews.com/news/2006/04/19/successful-trial-leads-to-nfc-deployment-by-nokia-philips-rmv-and-vodafone-in-hanau-germany/

[Cor06a] Cortesi A (2006) Prämienbonus für gesundes Leben? Tages-Anzeiger, 8. September 2006. Tamedia, Zürich, Schweiz

[Cor06b] Coroama V (2006) The Smart Tachograph – Individual Accounting of Traffic Costs and its Implications. In: Fishkin KP, Schiele B, Nixon P, Quigley A (eds.) Pervasive Computing – 4th International Conference, PERVASIVE 2006, Dublin, Ireland, May 7-10, 2006. Lecture Notes in Computer Science, vol 3968. Springer, Berlin Heidelberg New York, 135–152

[Cor06c] Coren G (2006) Shouldn't we tax fatties? Daily Mail Online, 27. Mai 2006. www.dailymail.co.uk/pages/live/articles/health/healthmain.html?in_article_id=388001&in_page_id=1774

[DaG02] Davies N, Gellersen H-W (2002) Beyond Prototypes: Challenges in Deploying Ubiquitous Systems. IEEE Pervasive Computing 1(1): 26–35

[DeM86] DeMarco T (1986) Controlling Software Projects: Management, Measurement, and Estimates. Prentice Hall, Upper Saddle River

[Das06] Das R (2006) RFID in retail – growing interest in item level. IDTechEx Website. www.idtechex.com/products/en/articles/00000479.asp

[Det06] Detecon Consulting (2006) Detecon warnt vor Gefahren für Kfz-Teile- und Zubehörgeschäft – RFID-gestütztes Ersatzteilmanagement stärkt Händler und das Markenbewusstsein von Autokäufern. Pressemitteilung, 23. Juni 2006. www.detecon.com/de/presse/presse_detail.php?press_id=1044

[Dwo05] Dworking G (2005) Paternalism. Stanford Encyclopedia of Philosophy, Online-Version, 20. Dezember 2005. plato.stanford.edu/entries/paternalism/

[Eco02] The Economist (2002) How about now? A survey of the real-time economy. The Economist, 2. Februar 2002. www.economist.com/displayStory.cfm?Story_id=949071

[Eco06] The Economist (2006) Soft paternalism: The state is looking after you. The Economist, 8. April 2006. www.economist.com/displaystory.cfm?story_id=6772346

[Edw05] Edwards R (2005) DNA test brings arrest for spitting at bus driver. The Evening Standard, News&Current Affairs. 6. April 2005. www.thisislondon.co.uk/news/article-17732278-details/DNA+test+brings+arrest+for+spitting+at+bus+driver/article.do

[Emn02a] TNS-Emnid (2002) Immer mehr Autofahrer wollen elektronischen Pfadfinder an Bord. www.tns-emnid.com/pdf/presse-presseinformationen/2002/2002_03_12_TNS_Emnid_Navigation.pdf

[Emn02b] TNS-Emnid (2002) Akzeptanz von Kundenkarten unter deutschen Verbrauchern. www.tns-emnid.com/pdf/presse-presseinformationen/2002/2002_04_26_TNS_Emnid_Kundenkarten.pdf

[Emn03] TNS-Emnid (2003) Bonusprogramme und Datenschutz – Verbraucher achten auf Sicherheit. www.tns-emnid.com/pdf/presse-presseinformationen/2003/2003_11_27_TNS_Emnid_Bonusprogramme.pdf

[Eur05] Eurotechnology (2005) Location based mobile services in Japan. Eurotechnology Japan, Juni 2005. eurotechnology.com/store/location/index.html

[Exx05] ExxonMobil Corporation (2005) Speedpass Fact Sheet. www2.exxonmobil.com/corporate/files/corporate/speedpass_fact_sheet.pdf

[FlM05] Fleisch E, Mattern F (2005) Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. Springer, Berlin Heidelberg New York

[Fre00] Frey J (2000) Progressive's "pay-as-you-drive" auto insurance poised for wide rollout. Insure.com Website, 18. Juli 2000. info.insure.com/auto/progressive700.html

[Fri97] Frisk D (1997) Beer and Nappies – A Data Mining Urban Legend. Private Website. web.onetel.net.uk/~hibou/Beer%20and%20Nappies.html

[FRNS+06] Frank C, Roduner C, Noda C, Sgroi M, Kellerer W (2006) Interfacing the Real World with Ubiquitous Gateways. Adjunct Proceedings of the 3rd European Workshop on Wireless Sensor Networks (EWSN 2006). www.vs.inf.ethz.ch/publ/papers/ewsn06.ubigate.pdf

[Goo04] Goo SK (2004) Sen. Kennedy Flagged by No-Fly List. The Washington Post, 20.08.2004, p A01. www.washingtonpost.com/wp-dyn/articles/A17073-2004Aug19 .html

[Goo05] Goo SK (2005) No-Fly Gaps Irk Airlines, DHS. The Washington Post, 25. Mai 2005, p A03. www.washingtonpost.com/wp-dyn/content/article/2005/05/24/AR2005052401388.html

[Gro00] Grob S (2000) Mit Videokamera gegen Autodiebe. Tages-Anzeiger, 27. Juni 2000. Tamedia, Zürich, Schweiz

[Haf06] Haffner P (2006) Die Zukunft geht unter die Haut. Das Magazin Nr. 39. Tamedia, Zürich, Schweiz

[HaS01] Harper J, Singleton S (2001) With a Grain of Salt – What Consumer Privacy Surveys Don't Tell Us. Studie des Competitive Enterprise Institutes (CEI), Juni 2001. www.cei.org/PDFs/with_a_grain_of_salt.pdf

[Hei06] Heise News (2006) Firma markiert Mitarbeiter per RFID. Heise News Online, 10. Februar 2006. www.heise.de/newsticker/meldung/69438

[Her06] Herrmann F (2006) Zwangsbetreuung für Asoziale geplant. RP Online, 2. September 2006. www.rp-online.de/public/article/nachrichten/politik/ausland/350160

[HeT02] Hempel L, Töpfer E (2002) Inception Report, Working Paper No. 1, UrbanEye Project. www.urbaneye.net/results/ue_wp1.pdf

[Him03] Himmelein G (2003) Ganz im Vertrauen – TCPA ist tot, es lebe die TCG. c't Magazin, 9/2003. www.heise.de/ct/03/09/052/

[Hos06] Hosein G (2006) Combatting Criminality in a World of Ambient Technology. Präsentation auf der Konferenz „Safeguards in a World of Ambient Intelligence", Brüssel, Belgien, 21.-22. März 2006. swami.jrc.es/pages/documents/SWAMI-Hosein20060321_ 000.pdf

[ICA04] International Civil Aviation Organization (2004) PKI for Machine Readable Travel Documents offering ICC Read-Only Access. Technical Report, Version 1.1, 1. Oktober 2004. www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf

[IDC06] IDC (2006) RFID Still in Early Stages in Western European Vertical Markets, but Adoption Increasing, Says IDC. IDC Pressemitteilung, 13. Januar 2006. www.idc.com/getdoc.jsp?containerId=pr2006_01_12_153428

[Joh06a] Johnston P (2006) Your Life in Their Lens. The Telegraph Online, 3. November 2006. www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/11/02/nspy202.xml

[Joh06b] Johnston P (2006) Britain: The Most Spied On Nation in the World. The Telegraph Online, 3. November 2006. www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/11/02/nspy02.xml

[Jor06] Jordan M (2006) Electronic Eye Grows Wider in Britain. Washington Post, Online Edition, 7. Januar 2006. www.washingtonpost.com/wp-dyn/content/article/2006/01/06/AR2006010602100.html

[Kan04] Kandel D (2004) Funkende Bücher – über 50 Bibliotheken im Vergleich. RFID-Forum, 1(2) 12–25. buecherei.netbib.de/coma/RfID/

[Küg05] Kügler D (2005) Risiko Reisepass. c't, 5/2005: 84–89

[Küp06] Küpper M (2006) Sicherheitsdebatte – Mehrheit wünscht sich Überwachungskameras. Spiegel Online, 18. August 2006, www.spiegel.de/politik/deutschland/0,1518,druck-432375,00.html

[Lan01] Langheinrich M (2001) Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In: Abowd GD, Brumitt B, Shafer S (eds.) Ubicomp 2001: Ubiquitous Computing – International Conference, Atlanta, Georgia, USA, September 30-October 2, 2001, Proceedings. Lecture Notes in Computer Science, vol 2201. Springer, Berlin Heidelberg New York, 273–291

[Lan05a] Langheinrich M (2005) Ortstermin im Land der Handys. Technology Review Online Edition, 15. September 2005. www.heise.de/tr/aktuell/meldung/63932

[Lan05b] Langheinrich M (2005) Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. In: [FlM05], 329–362. www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf

[Lan07] Langheinrich M (2007) RFID and Privacy. In: Petkovic M, Jonker W (eds.) Security, Privacy, and Trust in Modern Data Management. Springer, Berlin Heidelberg New York. www.vs.inf.ethz.ch/publ/papers/langhein2006rfidprivacy.pdf

[Lei06] Leicester University (2006) New University of Leicester study identifies links between musical tastes and lifestyle. Pressemitteilung, September 2006. www.eurekalert.org/pub_releases/2006-09/uol-nuo091206.php

[Les00] Lessig L (2000) Code and other laws of cyberspace. Basic Books, New York

[Les02] Lester W (2002) Americans historically trade liberties for security, pollsters say. Nando Times, 19. Mai 2002. www.cpfools.com/forum/showthread.php?t=640

[Let02] Lettice J (2002) Cap Cyborg to chip 11 year old in wake of UK child killings. The Register, 2. September 2002. www.theregister.co.uk/2002/09/02/cap_cyborg_to_chip/

[Let04] Lettice J (2004) Data on 10m Northwest fliers handed to NASA for 'testing'. The Register – Internet&Law, 20. Januar 2004. www.theregister.co.uk/2004/01/20/data_on_10m_northwest_fliers

[Let06] Lettice J (2006) How to clone the copy-friendly biometric passport. The Register – Internet&Law, 4. August 2006. www.theregister.co.uk/2006/08/04/cloning_epassports/

[Mac04] Mac Mathúna S (2004) Big Brother UK. *Flame* Online Magazin no 15. www.fantompowa.net/Flame/big_brotherUK.htm

[MaL01] Mattern F, Langheinrich M (2001) Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge. In: Müller G, Reichenbach M (Hrsg.) Sicherheitskonzepte für das Internet. Springer, Berlin Heidelberg New York, 7–26

[Mar03] Marx G (2003) Some Information Age Techno-Fallacies. Journal of Contingencies and Crisis Management, Vol 11, 25–31

[Mat03] Mattern F (2003) Total vernetzt – Szenarien einer informatisierten Welt. Springer, Berlin Heidelberg New York

[Mat05] Mattern F (2005) Die technische Basis für das Internet der Dinge. In: Fleisch E, Mattern F (Hrsg.): Das Internet der Dinge. Springer, Berlin Heidelberg New York, 39–66

[McN02] McCahill M, Norris C (2002) CCTV in London. UrbanEye Project, Working Paper No. 6, Juni 2002. www.urbaneye.net/results/ue_wp6.pdf

[NIS05] Niedersächsisches Ministerium für Inneres und Sport (2005) Niedersachsens Polizei testet Kennzeichenlesegeräte. Pressemitteilung, 2. Mai 2005. www.mi.niedersachsen.de/master/C10012482_L20_D0_I522_h1. html

[NKK01] National Public Radio, Henry J. Kaiser Family Foundation, Harvard University Kennedy School (2001) The 2001 NPR/Kaiser/Kennedy School Poll on Civil Liberties. www.npr.org/programs/specials/poll/civil_liberties/

[NZZ06] Neue Zürcher Zeitung (2006) Unklar, problematisch, unverhältnismässig – Das Hooligan-Gesetz aus der Sicht eines Datenschützers. NZZ Online, 12. Juni 2006. www.nzz.ch/2006/06/12/il/articleE71ZY.print.html

[Ren06] Rentrop C (2006) FID: Metro, Tesco und Wal-Mart feiern den Erfolg. Netzwelt.de-Website. www.netzwelt.de/news/69579_1-rfid-metro-tesco-und-walmart.html

[Rob05] Roberts P (2005) RFID crack raises spectre of weak encryption. Network World Website, 17. März 2005. www.networkworld.com/news/2005/0317rfidcrack.html

[Rod06] Roduner C (2006) The Mobile Phone as a Universal Interaction Device – Are There Limits? In: Rukzio E, Paolucci M, Finin T, Wisner P, Payne T (eds.) Proc. MobileHCI 2006 Workshop on Mobile Interaction with the Real World (MIRW 2006), 30–34

[Röt03] Rötzer F (2003) Kriegsgegner auf CAPPS-Überwachungsliste. Telepolis, 4. August 2003. www.heise.de/tp/r4/artikel/15/15375/1.html

[Röt05] Rötzer F (2005) Elektronische Fußfessel für Asylbewerber. Telepolis, 5. März 2005. www.heise.de/tp/r4/artikel/19/19597/1.html

[Röt06] Rötzer F (2006) Lebenslänglich wird jeder Schritt überwacht. Telepolis, 10. November 2006. www.heise.de/tp/r4/artikel/23/23941/1.html

[Sac06] Sachdave K (2006) Children arrested, DNA tested, interrogated and locked up... for playing in a tree. Daily Mail News, 23. Juli 2006. www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=397240

[Sch02a] Scheeres J (2002) Tech Keeps Tabs on School Kids. Wired News, 26. August 2002. www.wired.com/news/business/0,1367,54604,00.html

[Sch02b] Scheeres J (2002) Kidnapped? GPS to the Rescue. Wired News, 25. Januar 2002. www.wired.com/news/business/0,1367,50004,00.html

[Sch06a] Scheuch M (2006) Günstiger Drucker, teure Tinte. WISO Magazin, ZDF Online, 24. April 2006. www.zdf.de/ZDFde/inhalt/13/0,1872,3925965,00.html

[Sch06b] Schulzki-Haddouti C (2006) Videoüberwachung – Terrorkampf mit Gesichtskontrolle. Focus Online, 23. August 2006. focus.msn.de/digital/pc/videoueberwachung_nid_34165.html

[Sha03] Shabi R (2003) The Card Up Their Sleeve. The Guardian, 19. Juli 2003, www.guardian.co.uk/weekend/story/0,3605,999866,00.html

[Sla04] Slashdot News (2004) ZeroKnowledge to Discontinue Anonymity Service. User Posting, 4. Oktober 2004. slashdot.org/yro/01/10/04/1526256.shtml

[Slo10] Sloss R (1910) Das drahtlose Jahrhundert. In: Brehmer A (Hrsg.) Die Welt in 100 Jahren. Verlagsanstalt Buntdruck, Berlin

[SoR03] Solove D, Rotenberg M (2003) Information Privacy Law. Aspen Publishers, New York

[Spi02] Der Spiegel (2002) Autokennzeichen-Scanner – Becksteins neustes Spielzeug. Spiegel Online, 2. Dez. 2002. www.spiegel.de/auto/aktuell/0,1518,224854,00. html

[Spi06a] Der Spiegel (2006) Internet – Voyeure im Netz. 2006(10): 147

[Spi06b] Der Spiegel (2006) Generation Praktikum. 2006(31): 44–49

[Spi06c] Der Spiegel (2006) Panorama – Auf Nummer Sicher. 2006(9): 20

[Spi06d] Der Spiegel (2006) Panorama – Terrorgefahr: Deutsche fürchten keine Anschläge. Spiegel Online, 28. August 2006. www.spiegel.de/panorama/0,1518,433497,00.html

[SpP07] Spiekermann S, Pallas F (2007) Technologiepaternalismus – Soziale Auswirkungen des Ubiquitous Computing jenseits der Privatsphäre. In: Mattern F (Hrsg.) Die Informatisierung des Alltags. Leben in smarten Umgebungen. Springer, Berlin Heidelberg New York

[Sta06] Stallman R (2006) Can you trust your computer? Online Essay, 6. Juni 2006. www.gnu.org/philosophy/can-you-trust.html

[StW04] StateWatch (2004) UK: Police can keep DNA of innocent people indefinitely. StateWatch.org, Juli 2004. www.statewatch.org/news/2004/sep/03uk-dna-database.htm

[StZ06] Stadtschreiber Stadt Zürich (2006) Auszug aus dem Protokoll des Stadtrates von Zürich, GR Nr. 2005/457. Stadt Zürich, 5. April 2006. www.gemeinderat-zuerich.ch/DocumentLoader.aspx?ID=34ffff3a-d3fb-4d2d-9b13-45faea9750a6.pdf&Title=2005_0457.pdf

[Swi06] Swinford S (2006) Asbo TV helps residents watch out. The Sunday Times Online, 8. Januar 2006. www.timesonline.co.uk/article/0,,2087-1974974,00.html

[Tan06] Tan A (2006) RFID spills the beans on Samsung Tesco shoppers. ZDNet Asia News, 4. Juli 2006. networks.silicon.com/lans/0,39024663,39160095,00.htm

[ThG05] Thiesse F, Gillert F (2005) Das smarte Buch. In [FlM05], 291–299

[TMC05] Technology Marketing Corporation TMC (2005) Worldwide RFID Spending to Surpass $3 Billion in 2010. Pressemitteilung, 13. Dezember 2005. www.tmcnet.com/usubmit/2005/dec/1221397.htm

[Trö07] Tröster G (2007) Kleidsamer Gesundheitsassistent – Computer am Körper, im Körper. In: Mattern F (Hrsg.) Die Informatisierung des Alltags. Leben in smarten Umgebungen. Springer, Berlin Heidelberg New York

[Van00] Vanderlippe J (2000) What Savings? C.A.S.P.I.A.N Website, Mai 2000. www.nocards.org/savings/krogerads.shtml

[VDA99] Verband der Automobilindustrie (1999) Jahresbericht Auto 1999. www.vda.de/de/service/jahresbericht/files/vda_99.pdf

[VDA06] Verband der Automobilindustrie (2006) Jahresbericht Auto 2006. www.vda.de/de/service/jahresbericht/files/VDA_2006.pdf

[Vog98] Vogel J (1998) When cards come collecting – How Safeway's new discount cards can be used against you. Seattle Weekly, September 24-30, 1998. www.seattleweekly.com/news/9838/features-vogel.php

[VZB03] Verbraucherzentrale Bundesverband e.V. (2003) Kundenbindungssysteme und Datenschutz. Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. www.vzbv.de/mediapics/gutachten_kundenbindungssysteme_2003.pdf

[War06] Warwick K (2006) Wiring in Humans – Advantages and problems as humans become part of the machine network via implants. Vortrag und Diskussion auf der „Conference on safeguards in a world of ambient intelligence" am 21. März 2006, Brüssel, Belgien. swami.jrc.es/pages/Conference2006.htm

[Wei91] Weiser M (1991) The computer for the 21st century. Scientific American, 265(3): 66–75. Reprinted in IEEE Pervasive Computing, 1(1), Jan.-Mar. 2002: 19–25.

[Wei93] Weiser M (1993) Some Computer Science Issues in Ubiquitous Computing. Communications of the ACM 36(7): 75–85

[Wei99] Weiser M, Gold R, Brown JS (1999) The origins of ubiquitous computing research at PARC in the late 1980s. IBM Systems Journal 38(4): 693–696

[Wes05] Westhues J (2005) Hacking the Prox Card. In: Garfinkel S, Rosenberg B (eds.) RFID. Applications, Security, and Privacy. Addison-Wesley, Boston. Siehe auch http://cq.cx/verichip.pl und http://cq.cx/vchdiy.pl

[Wik06a] Wikipedia contributors (2006) Super Urban Intelligent Card. Wikipedia, die freie Enzyklopädie. Bearbeitungsstand: 5. Juni 2006, 10:19 UTC. de.wikipedia.org/w/index.php?title=Super_Urban_Intelligent_Card&oldid=17490641

[Wik06b] Wikipedia contributors (2006) UK National DNA Database. Wikipedia, The Free Encyclopedia. Bearbeitungsstand: 10. Oktober 2006, 11:59 UTC. en.wikipedia.org/w/index.php?title=UK_National_DNA_Database&oldid=80599989

[Yua06] Yuan L (2006) Do you know where your children are? These gadgets help. Wall Street Journal, 27. April 2006. www.post-gazette.com/pg/06117/685620-51.stm

[Zei04] Zeidler M (2004) RFID: Der Schnüffel-Chip im Joghurtbecher. Monitor Magazin, Köln, 8. Januar 2004. www.wdr.de/tv/monitor/beitrag.phtml?bid=554&sid= 108

[ZKSB02] Zurko ME, Kaufman C, Spanbauer K, Bassett C (2002) Did You Ever Have to Make Up Your Mind? What Notes-Users Do When Faced with a Security Decision. In: Notargiacomo L, Thomsen D (eds.) Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC 2002), IEEE Press, Piscataway, 371–381

[Zur04] Zurawski N (2004) „Die Kameras stören mich nicht!" Telepolis, 20. Januar 2004. www.heise.de/tp/r4/artikel/16/16542/1.html

Dr. Marc Langheinrich ist Oberassistent am Institut für Pervasive Computing der ETH Zürich. Er studierte an der Universität Bielefeld und der University of Washington in Seattle (USA) Informatik und promovierte 2005 an der ETH Zürich (Thema: Privacy in Ubiquitous Computing – Tools and System Support). 1996-1997 arbeitete er für das Office for Naval Research in Seattle, 1997-1999 war er Forscher in der Multimedia-Gruppe des zentralen NEC-Forschungszentrums in Kawasaki (Japan). Seit Ende 1999 ist er Mitglied der Gruppe „Verteilte Systeme“ von Prof. Dr. Friedemann Mattern an der ETH Zürich. Marc Langheinrich arbeitet seit 1997 an technischen Datenschutzlösungen – er ist Mitautor der P3P-Spezifikation, dem De-facto-Standard für maschinenlesbare Privacy-Policies im World-Wide-Web, Mitglied des Editoral Boards des Journals of Privacy Technology (JOPT) und Autor zahlreicher Konferenz- und Zeitschriftenbeiträge zum Thema Datenschutz und Privatsphäre.