1 Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge

Friedemann Mattern, ETH Zürich
Marc Langheinrich, ETH Zürich

Mit der weiter zunehmenden Miniaturisierung der Computertechnologie werden in absehbarer Zukunft Prozessoren und kleinste Sensoren mehr und mehr in Alltagsgegenstände integriert, wobei die traditionellen Ein- und Ausgabemedien von PCs, wie etwa Tastatur, Maus und Bildschirm, verschwinden und wir stattdessen „direkt" mit unseren Kleidern, Armbanduhren, Schreibstiften, Regenschirmen oder Möbeln kommunizieren (und diese wiederum untereinander und mit den Gegenständen anderer Personen).

Solch eine Entwicklung hat nicht nur weit reichende Konsequenzen in traditionellen Gebieten der praktischen Informatik, welche z.B. Effizienz, Nutzbarkeit und Skalierbarkeit solcher massiv verteilten Systeme zu verbessern versucht, sondern erfordert auch intensive Anstrengungen auf den Gebieten Sicherheit und Datenschutz, um diese schöne neue Welt voller „smarter" und kommunikationsfreudiger Dinge nicht in einen orwellschen Überwachungsstaat zu verwandeln [Bri].

1.1 Der unsichtbare Computer

Der Begriff des allgegenwärtigen Computers, *Ubiquitous Computing*, wurde bereits 1988 von dem 1999 früh verstorbenen Mark Weiser, seinerzeit leitender Wissenschaftler am Xerox Palo Alto Research Center (PARC), geprägt. Nach Weisers Auffassung sollte der Computer reines Mittel zum Zweck sein, eine bestimmte Aufgabe durch Konzentration auf das eigentliche Problem zu lösen – der

XEROX-Forscher Mark Weiser prägte 1988 den Begriff „*Ubiquitous Computing*"

universelle PC mit Tastatur und Maus steht dabei eher im Wege, da er durch seine Komplexität die Aufmerksamkeit des Benutzers über Gebühren strapaziert [Wei].

Die „Post-PC-Ära": Internet und Mobilkommunikation wachsen zusammen

WAP-fähige Handys, mit dem Internet verbundene Spielkonsolen und drahtlos kommunizierende PDAs sind erste Vorboten dieser von Weiser beschworenen „Post-PC-Ära", welche sich für den Benutzer vor allem dadurch manifestiert, dass das Internet mit Mobilkommunikationssystemen (wie z.B. UMTS) zusammenwächst und dass mehr und mehr PC-Anwendungen in kleine, spezialisierte „information appliances" abwandern, was den Gebrauch der Funktionalität für den Nutzer drastisch vereinfachen sollte [Nor].

1.1.1 Technische Grundlagen

Moores Gesetz: Chip-Leistung verdoppelt sich alle 18 Monate

Grundlage der visionären Ansichten vieler Technologieexperten ist die Tatsache, dass der Fortschritt in der Informationstechnik auch weiterhin ungebrochen dem mooreschen Gesetz zu folgen scheint, welches bereits seit mehreren Jahrzehnten recht präzise voraussagt, dass sich die Leistungsfähigkeit von Prozessoren alle 18 Monate verdoppelt. Speichermedien und Kommunikationsbandbreite weisen derzeit sogar eine noch höhere Steigerungsrate auf. Experten gehen davon aus, dass dies auch noch eine ganze Reihe von Jahren so weitergehen wird. Dies und Fortschritte in den Materialwissenschaften (z.B. Miniatursensoren, „elektronische Tinte" oder „leuchtendes Plastik") lassen die Annahme zu, dass unsere nahe Zukunft voll sein wird von kleinsten, spontan miteinander kommunizierenden Rechnern, welche aufgrund ihrer geringen Größe und ihres vernachlässigbaren Preises leicht in Alltagsgegenstände integriert und dadurch kaum mehr als Computer im heutigen Sinne wahrgenommen werden [Han, Mat].

Internet überall

Bereits jetzt genießen tragbare und drahtlos mit dem Internet verbundene Geräte eine große Aufmerksamkeit der Computerindustrie. Bald dürfte jedwedes technische Gerät – vom Laptop über den PDA hin zum elektronischen Buch, vom Auto bis zum Telefon – ganz selbstverständlich das Internet mit seinen vielfältigen Ressourcen für die Durchführung seiner Aufgaben mit einbeziehen, auch wenn sich die Nutzer selbst dieses Umstands oft gar nicht bewusst sind.

Eine „smarte" Umwelt aus Sensoren und unsichtbaren Computern

Immer kleiner werdende Sensoren, vom einfachen Temperaturfühler und Lichtsensor hin zum Druck- oder Beschleunigungsmesser, zusammen mit immer leistungsstärkeren Prozessoren und Batterien ermöglichen eine immer umfassendere Erfassung und automatische Wahrnehmung der Umwelt. Sei es durch stationäre Installation

an Fassaden, Türen oder Einrichtungsgegenständen, sei es durch Integration in verschiedenste Alltagsgegenstände wie Möbel, Armaturen, Kleidung oder Accessoires – die uns umgebende Umwelt wird „smart“ werden und über ihre ursprüngliche Funktionalität hinaus eine breite Palette zusätzlicher wünschenswerter (oder auch überflüssiger) „Services“ anbieten können: Die Kaffeemaschine, die zusammen mit Tasse und Zuckerdose unsere tägliche Zufuhr an Koffein und Zucker überwacht und uns bei zu starkem Konsum zu entkoffeiniertem Kaffee mit Süßstoff rät. Oder die Sonnenbrille, die uns beim zufälligen Treffen eines alten Bekannten durch das Einblenden dessen Vornamens auf die Sprünge hilft. Oder das Gebäude, welches uns auf der Suche nach dem richtigen Büro im richtigen Stockwerk den Fahrstuhl anhält.

Gegenstände der Zukunft kooperieren und kommunizieren miteinander

Prinzipiell jedenfalls werden die Gegenstände der Zukunft mittels spontaner Vernetzung und intelligenter Kooperation Zugriff auf jegliche in Datenbanken oder im Internet gespeicherte Information besitzen bzw. jeden passenden Internet-basierten Service nutzen können. Die Grenzen liegen weniger in der technischen Natur, sondern sind allenfalls ökonomischer (was darf der Zugriff auf eine bestimmte Information kosten?) oder rechtlicher Art (was darf der Gegenstand wem verraten?).

Neue Materialien verändern das Bild des Computers

Weitere Fortschritte in den Materialwissenschaften beginnen, auch das äußere Erscheinungsbild des Computers drastisch zu verändern: Statt Schreibmaschinentastatur und Röhrenstrahl-Monitor stehen heute schon an vielen Arbeitsplätzen Mikrofon und Flachbildschirm. Neuartige Werkstoffe und Techniken werden in Form faltbarer Bildschirme aus dünnem Plastik und Laser-Projektionen aus der Brille direkt auf die Netzhaut des Auges traditionelle Ausgabemedien weiter verdrängen. Flach in die Tapete integriert, zusammengefaltet in der Tasche oder in die Umgebung projiziert – Informationen können überall und jederzeit zugänglich gemacht werden, idealerweise ohne unsere momentane Tätigkeit zu beeinträchtigen. So wird beispielsweise intensiv an „elektronischer Tinte“ geforscht, welche Papier und Stift zum vollwertigen, hoch mobilen Ein- und Ausgabemedium mit einer uns gut vertrauten Nutzungsschnittstelle erhebt. Der Computer als Gerät ist dann verschwunden – er ist eine Symbiose mit den Dingen der Umwelt eingegangen und wird höchstens noch als eine unsichtbare Hintergrundassistenz wahrgenommen.

1.1.2 Herausforderungen

Neue Herausforderungen an die Informatik

In der praktischen und angewandten Informatikforschung ergibt sich durch die erwartete Allgegenwärtigkeit des Computers eine Vielzahl von Herausforderungen – sowohl in den Einzeldisziplinen als auch im komplexen Zusammenspiel der verschiedenen Aspekte. Kommunikationsprotokolle, Routingverfahren und Quality of Service müssen plötzlich in Dimensionen betrachtet werden, gegen die das heutige Internet mit seinen Millionen von Rechnern geradezu überschaubar wirkt. Der darüber hinaus stark zunehmende Grad an Mobilität, Dynamik und Heterogenität erfordert weitere Maßnahmen. Auch beim Software-Engineering und allgemein beim Systementwurf muss umgedacht werden: Schon aus Kosten- und Platzgründen werden Systemressourcen oft sehr begrenzt, und elektrische Energie ein knappes Gut sein. Und da es keinen Systemverwalter geben kann, der alle unsere „smarten" Gegenstände ständig wartet, erzwingt dies geradezu neue Lösungen für „plug & play", automatische Synchronisation und Fehlertoleranz.

Doch neben den oben genannten, weitgehend technischen Aspekten wirft das Ubiquitous Computing auch neue, grundlegende Fragen auf, die weit über das klassische Gebiet der praktischen Informatik hinaus gehen: Wie lassen sich die Unmengen durch smarte Dinge und Sensoren generierten Daten strukturieren, damit Anwendungen, die man in einer offenen Welt nicht alle kennen kann, davon profitieren können? Oder: Wie interagiert man eigentlich mit einem unsichtbaren Computer? Oder etwa: Wie lässt sich das Datenschutzproblem angehen, wenn unsere persönlichen Dinge personenbezogene Daten erzeugen und diese kommunizieren – und zwar ohne dass dazu jeder gleich zum Sicherheitsexperten werden muss?

Privatsphäre trotz ubiquitärer Überwachungsinfrastruktur?

Letzteres ist sicherlich eines der am schwerwiegendsten Probleme: Schlechte Benutzerschnittstellen sind allenfalls störend und werden schlimmstenfalls eine kommerzielle „Karriere" solcher Geräte und „intelligenter" Gegenstände behindern. Strukturierte, interoperable Datenmodelle vermeiden zwar Insellösungen einzelner Hersteller, doch haben wir bereits seit dutzenden von Jahren gelernt, mit Inkompatibilitäten zu leben. Aber ohne effektive Maßnahmen zum Datenschutz erschaffen wir mit Ubiquitous Computing in kürzester Zeit eine Überwachungsinfrastruktur, welche viele bestehenden Gesetze und Mechanismen zum Schutze der Privatsphäre des Einzelnen ad absurdum führen oder ineffektiv und nutzlos machen könnte.

„Forget privacy"?

Es mag in diesem Zusammenhang etwas zynisch klingen, ist aber wohl ernst gemeint, wenn die Gartner-Unternehmensberatung in einer neuen Analyse unter dem Begriff „Insight for the Connected World" (bei der es um „Emerging High-Impact Trends" geht) u.a. schreibt: „By 2010, driven by the improving capabilities of data analysis... privacy will become a meaningless concept in Western societies." Ist es da tröstlich, wenn die Analytiker diesem in einer Bewertung „nur" eine Wahrscheinlichkeit von 60% zuordnen? Manche Forscher jedenfalls scheinen vor den technischen Aussichten eher zu kapitulieren: Bei einer Podiumsdiskussion, die im Herbst 2000 zum Thema „Security and Privacy in Ubiquitous Computing Environments" im Rahmen der Fachtagung „Handheld and Ubiquitous Computing" stattfand [HUC], sagte einer der Teilnehmer wörtlich „forget privacy"! Diese „These" wurde von ihm dann mit Vehemenz während der ganzen Podiumsdiskussion vertreten. Müssen wir also wirklich kapitulieren? Oder gibt es zumindest Ansätze für eine Lösung?

1.2 Datenschutz in Ubiquitären Systemen?

„Privacy is an illusion; we haven't had any for twenty years. All that's left is in your head – maybe that's enough." (Aus dem Film "Enemy of the State")

Mit dem Aufkommen und rapiden Wachstum des Internets und seines populärsten Dienstes, dem World-Wide-Web (WWW), hat sich die Datenschutz-Landschaft in den letzten Jahren stark verändert. Wo vorher meist staatliche Stellen mit ihrem Hang zur detaillierten Kontrolle über den Bürger umfangreiche Dossiers in zentralen Datenbanken erstellten (z.B. durch Sozialämter zur Kontrolle der Beihilfezahlung, oder durch die Polizei für eine verbesserte Strafverfolgung), droht inzwischen Gefahr durch viele fragmentierte, kommerzielle Datensammlungen, welche der Einzelne im täglichen Umgang mit hoch technisierten Dienstleistungen kontinuierlich füllt: Verbindungsnachweise beim Telefonieren mit ISDN, Einkaufsgewohnheiten beim Online-Shopping oder dem Einkauf mit der Prämienkarte des Supermarktes, Bewegungsmuster bei Verwendung von Kreditkarte oder Mobiltelefon, oder sogar detaillierte Korrespondenz bei Teilnahme an Online-Foren und News-Gruppen.

Datenschutzproblematik im WWW

Dass vom „harmlosen" Surfen im Web Gefahr für die Privatsphäre droht, ist langjährigen Benutzern des Internets längst bekannt, vielen Neulingen jedoch nicht immer bewusst. Jeder Abruf einer Web-Seite wird von ihren Anbietern protokolliert, archiviert und oftmals zwecks Angebotsoptimierung analysiert. Kleine Identifikationsmarker, *Cookies* genannt, können dem Besucher einer Web-Site unbemerkt zugewiesen werden – beim nächsten Besuch identifiziert

sich der Web-Browser des Benutzers dann automatisch mit diesem Marker beim Anbieter. Hinterlässt der Besucher bei einem dieser Besuche seinen Namen oder sonstige personenbezogene Informationen (z.B. beim Ausfüllen von Antragsformularen, der Aufgabe von Bestellungen, oder auch nur bei der Auswahl des persönlichen Horoskops), können diese leicht mit dem *Cookie* des Web-Browsers verknüpft werden und identifizieren so den Benutzer bei allen folgenden (und vorausgegangenen) Besuchen.

Online-Historie erlaubt Einblick in das Alltagsleben

Auf diese Weise akkumuliert sich schnell eine umfassende Online-Historie, sehr oft ohne dass Benutzer sich darüber im Klaren sind. Dabei bedeutet „Online" nicht unbedingt, dass diese Daten keinen Bezug zum „Offline", zur realen Welt des Benutzers, hätten: Online-Daten wie beispielsweise Diskussionsbeiträge in News-Gruppen oder Suchbegriffe in Web-Verzeichnissen erlauben sehr oft einen detaillierten Blick in das Alltagsleben des Benutzers.

Obwohl die Aufteilung dieser Daten auf eine Vielzahl von Anbietern im ersten Moment im Sinne des Datenschutzes vorteilhaft erscheint, ist dies nicht wirklich als Fortschritt gegenüber den staatlichen, zentralistischen Strukturen der 70er-Jahre anzusehen. Während zentrale Datensammlungen zwar das Missbrauchspotential erhöhen (ein Unberechtigter kann sich weitaus schneller weitaus mehr Informationen verschaffen), verstärken sie doch gleichzeitig auch die Sicherheit (Zugangskontrollen lassen sich leichter implementieren) und erleichtern die Korrektur oder Löschung fehlerhafter Daten. Eine anfängliche Fragmentierung ist jedenfalls kein Garant dafür, dass verteilte Daten nicht zu einem späteren Zeitpunkt wieder zusammengeführt werden: Dafür sorgen allein schon die konsequente elektronische Verfügbarkeit sowie weltweit verbreitete Datenbank-Standards wie SQL oder universelle Datenbeschreibungsformate wie XML. Viele Online-Firmen, die in Folge der Kurskorrekturen an der Börse im Verlauf des Jahres 2000 Konkurs anmelden mussten, haben bereits ihre Kundenkartei als wertvolle Handelsware erkannt [Gar].

Die reale Welt geht online

Die Vision des allgegenwärtigen Computers erweitert die Datensammlung nun zur umfassenden Offline-Historie: Während sich in den meisten Fällen die Web-Überwachung für den Benutzer klar abgrenzbar auf die Benutzung von PCs beschränkt, wird es in einer Welt voll „smarter" Alltagsgegenstände oft gar keine Unterscheidung zwischen „Online" und „Offline" mehr geben. „Smarte" Möbel und Kleidungsstücke werden fast immer aktiv sein und selbst in den eigenen vier Wänden genau wahrnehmen können, was man gerade tut. Intelligente Bürogebäude, die Besucher automatisch zum richtigen Büro führen und den Aufenthaltsort des Firmenausweises

(und damit in der Regel auch den Aufenthaltsort des Inhabers) kennen, verfügen über detaillierte Bewegungs- und Interaktionsmuster, sowohl für Angestellte als auch für vorübergehende Besucher. Informations- und Navigationseinrichtungen auf öffentlichen Plätzen weisen Touristen auf Sehenswürdigkeiten und Einheimische auf die Abfahrtszeiten im öffentlichen Nahverkehr hin, und wissen so oft implizit, was Besucher sehen wollten und wer wie wohin fuhr.

Datenspuren in der realen Welt

Durch diese Aufhebung der strikten Trennung zwischen Online und Offline gewinnen die allgegenwärtig erhobenen Daten zwangsweise an Qualität: Wo vorher nur ein relativ kleiner Teil meiner Person durch Stöbern in den Datenspuren erfassbar schien (nämlich die Zeit, die ich bei der Verfolgung meiner beruflichen und privaten Interessen online verbrachte), offenbart sich in der ubiquitären Vision ein weitaus detaillierteres Bild über meine Neigungen, Hobbys, meine allgemeine Verfassung und vor allem auch über meine Schwächen.

Personalisierung verdrängt Anonymität

Besonders kritisch erscheint, dass die Grenze zwischen „personenbezogenen“ und „anonymen“ Daten bei einer derart stark zunehmenden Datenmenge verschwimmt, da immer leistungsfähigere Rechner und Verfahren die nachträgliche Korrelation solcher Informationen erleichtern. Die zunehmende Personalisierung, vor allem auch bei der Angebots- und Preisgestaltung, verstärkt diesen Effekt noch, da anonyme Spuren immer individueller werden. So könnte etwa aus einer Vielzahl anonymer Tankquittungen, die jedoch einen speziellen Angebotspreis für Vielfahrer aus dem Vorstadt-Gebiet mit einer Vorliebe für eine bestimmte Zigarettenmarke aufweisen, leicht ein detailliertes Bewegungsmuster für eine ganz bestimmte Person destilliert werden. Je individueller und personalisierter unsere Welt wird, desto persönlicher werden auch an sich anonyme Informationen werden. Ubiquitous Computing mit seiner Allgegenwärtigkeit des Computers erleichtert nun aber Individualisierung und Personalisierung, hat sie sogar oft zum Zweck und verschärft daher die damit einhergehende Datenschutzproblematik wesentlich.

1.2.1 Grundlagen für die Wahrung der Privatsphäre

Auf welche Aspekte müssen wir unser Augenmerk richten, wenn wir in einer Welt voller kommunizierender Alltagsgegenstände nicht unweigerlich zum „gläsernen Menschen“ werden wollen? Was sind die Zutaten, die einen effektiven Datenschutz in einer solchen Zukunft möglich machen? Sicherlich können wir von den Erfahrungen, die seit dem Aufkommen der elektronischen Datenverarbeitung

gemacht wurden, profitieren, auch wenn viele Schwerpunkte in Zukunft anders gesetzt werden müssen. Vor allem die jüngsten Entwicklungen im Web erlauben in begrenztem Masse eine Extrapolation auf die Aspekte, die mit dem Ubiquitous Computing relevant werden, und können uns so als Denkanstoß, wenn nicht sogar als Blaupause, für kommende Datenschutzbestrebungen dienen.

E-Privacy

Leicht lassen sich im aufkommenden Online-Handel vier Hauptaspekte identifizieren, welche für eine die Privatsphäre des Einzelnen respektierende E-Commerce-Umgebung unabdingbar sind und so die Grundbausteine einer „E-Privacy“ [Bäu] darstellen:

- *Anonymität***:** Wie kann ich meinen Namen und andere personenbezogene Daten über mich verbergen bzw. nur selektiv preisgeben?
- *Vertraulichkeit*: Wie kann ich sicherstellen, dass unbefugte Dritte keinen Zugriff auf meine Daten haben – sowohl während der Übertragung als auch danach?
- *Transparenz***:** Wie kann ich mir darüber im Klaren sein, welcher Aspekt meiner Person (Bewegungsmuster, Diskussionsbeiträge, etc.) zu irgendeinem Zeitpunkt überwacht wird, und unter welchen Umständen (d.h. Grund der Überwachung, Dauer der Datenspeicherung, Empfänger der Daten, etc.) dies geschieht?
- *Vertrauen und Absicherung***:** Wem kann ich vertrauen, dass Abmachungen (d.h. über Grund und Umfang der Datensammlung und deren Empfänger) eingehalten werden, und wer kann mir im Konfliktfall helfen?

Es ist sehr wahrscheinlich, dass diese Aspekte auch bei Lösungen für „M-Privacy“ (also in einer M-Commerce-Umgebung) bis hin zur „U-Privacy“ (Ubiquitous Privacy – Datenschutz in ubiquitären Umgebungen) eine wichtige Rolle spielen werden, auch wenn die Qualität der Daten in den einzelnen Szenarien stark unterschiedlich ist. Im Einzelnen gilt es zu überlegen, welche Lösungsansätze bereits für jeden dieser vier Bereiche im Web existieren, und inwiefern sie sich auf zukünftige ubiquitäre Szenarien übertragen lassen. Dies wird in den nachfolgenden Kapiteln diskutiert.

1.2.2 Anonymität und Vertraulichkeit

Eine Vielzahl von Werkzeugen steht derzeit dem technisch versierten Web-Surfer zur Verfügung, um seine Datenspuren im Internet zu verwischen: Anonymisierungs-Dienste wie Anonymizer.com oder

die „Freedom“-Software der kanadischen Firma Zero-Knowledge ermöglichen dank ausgeklügelter Technik, dass beim Abruf einer Web-Seite die eigene Internet-Adresse geheim gehalten wird. Verschlüsselungsprogramme und -protokolle wie PGP, SSH und SSL erlauben das Sichern von Information bei der Übermittlung zwischen zwei Computern, so dass Lauscher keine Abhörmöglichkeit haben.

Mobile Vertraulichkeit

Während im Web Anonymisierung und sichere Verbindungen immer mehr genutzt werden, ist in mobilen Umgebungen, also beim M-Commerce, beides nur schwerer zu erreichen. Dies liegt zum einen in den begrenzten Ressourcen (z.B. bezüglich Bandbreite und Rechenleistung) der mobilen Geräte, zum anderen an der in vielen Ländern vom Gesetzgeber geforderten polizei- und geheimdienstlichen Abhörbarkeit für mobile Gespräche, welche z.B. im Falle des GSM-Standards die Verschlüsselungsalgorithmen so weit verwässerten, dass sie heutzutage nach Expertenmeinung bereits mit einem handelsüblichen PC in Echtzeit entschlüsselt werden können. Nicht zuletzt deshalb wird im WAP-Standard mit WTLS ein zusätzliches Sicherheitsprotokoll definiert, welches aber ebenfalls einige Schwachstellen besitzt: Zum einen ist der Einsatz von WTLS optional und kann vom Benutzer nicht leicht überprüft werden, zum anderen muss aufgrund der unterschiedlichen Standards in Fest- und Mobilnetz in so genannten *Gateway*-Rechnern zwischen WTLS und SSL übersetzt werden, wodurch die Nachricht, wenn auch nur kurzzeitig, im Klartext offen gelegt wird.

Vertraulichkeit in drahtlosen Kommunikationsprotokollen

Drahtlose Kommunikationsprotokolle für lokale Netze wie WLAN und Bluetooth bieten kaum nennenswerte Verbesserungen. Zwar definiert der IEEE802.11 Standard mit WEP („Wired Equivalent Privacy“) eine sichere Verbindung auf Link-Ebene, doch ist diese nur mit relativ schwachen 40-Bit Schlüsseln auf Hop-by-Hop-Basis (statt End-to-End, d.h. auf der gesamten Verbindung zwischen Endgerät und Anbieter) gesichert. Im Bluetooth-Standard muss sich jedes Gerät mit seiner *Unique Device Address* identifizieren, welches Anonymität unmöglich macht. Eine per Voreinstellung lediglich auf einem 4-stelligen PIN basierende Verschlüsselung ist ferner für vertrauliche Daten höchst ungeeignet. Verlässliche Verschlüsselung muss also sowohl im 802.11 Standard als auch bei Bluetooth auf höher gelegenen Ebenen (z.B. auf Network-, Transport- oder Anwendungsebene) geschehen. Im zukünftigen IPv6 Standard beispielsweise, der bald den heutigen IPv4 Standard ablösen soll, wird das Konzept des „Encapsulated Security Payload“ definiert, welches sowohl komplette Datagramme (im „Tunnel-Mode“) als auch nur den Paketinhalt (Payload-Verschlüsselung im „Transport-Mode“)

direkt auf dem Network-Layer verschlüsselt. Dies ermöglicht End-to-End-Sicherheit, welche durch Integration auf niedrigerer Ebene potentiell mächtiger als eine Verschlüsselung auf Transport-Ebene (wie z.B. SSL) sein kann.

Low-Power gleich Low-Security?

Ubiquitären Anwendungen, die Anonymität und Vertraulichkeit bereits frühzeitig in der Design-Phase integrieren wollen, mangelt es sicher nicht an dem nötigen kryptographischen Handwerkszeug. Viele der oben beschriebenen Basistechnologien bieten bereits eine ganze Reihe von Sicherheitsaspekten, welche durch geschickte Kombination einen effektiven Schutz versprechen können. Weitaus problematischer werden sich aber womöglich die physikalischen Nebenbedingungen auswirken, welche einen Einsatz von komplexen Sicherheitsverfahren und -protokollen in Low-Power-Umgebungen erschweren [Tim].

Vertraulichkeit braucht Authentizität

Vertraulichkeit bedeutet aber auch Authentizität: Nur wenn ich sicher sein kann, dass der Absender auch wirklich der ist, für den er sich ausgibt, kann ich meine Daten mit gutem Gewissen herausgeben. Public-Key-Verfahren erlauben dies heute schon in begrenztem Maße auf dem Web, wo Firmen wie Thawte oder Verisign digitale Schlüssel zertifizieren, mit denen dynamische Web-Inhalte und Programme signiert werden können. Viele Systeme und Protokolle weisen aber noch Unzulänglichkeiten auf: Beim WEP-Protokoll („Wired Equivalent Privacy“) des IEEE802.11 LAN-Standards können lediglich ganz Gruppen von Geräten authentisiert werden, was eine Unterscheidung zwischen Geräten einer Gruppe, z.B. für einen differenzierteren Zugang, unmöglich macht. IPv6 bietet zwar „Authentication Headers“ zur verbesserten Authentisierung von Nachrichten an, deren Schwerpunkt jedoch eher auf der Unverfälschbarkeit der Daten, als auf deren Nichtabstreitbarkeit und Authentizität liegt. Letzteres muss auch in IPv6 auf höher gelegenen Ebenen geschehen. Zwar können hierfür die vom Web bekannten Zertifizierungssysteme verwendet werden, doch bleibt fraglich, wie sich diese Strukturen in ubiquitären Umgebungen skalieren lassen.

Während im M-Commerce die Authentisierung noch zentral vom Netzbetreiber durchgeführt wird, müssen zukünftige Lösungen Zertifizierung auch lokal für Privatpersonen zugänglich machen – schließlich möchte man nicht jede Kaffeetasse vor Gebrauch erst bei einer zentralen Stelle anmelden müssen. Das für E-Mail gebräuchliche Verschlüsselungsprogramm PGP geht hier mit gutem Beispiel voran: Anwender zertifizieren sich gegenseitig, d.h. ohne zentrale Verwaltung, und machen die Vertrauenswürdigkeit eines Zertifikates von dessen Empfehlungen abhängig. Problematisch ist dabei allerdings die Granularität: Nur wenn sich genügend Anwender an

der gegenseitigen Zertifizierung beteiligen, besteht eine reelle Möglichkeit, unbekannte Zertifikate entlang solcher Empfehlungsketten auf vertrauenswürdige Empfehlungen von Freunden und Kollegen zurückverfolgen zu können. Die besondere Anforderung von ubiquitären Systemen nach komfortablen Administrationsschnittstellen wird sich dabei ebenfalls erschwerend bemerkbar machen: bei mehreren Dutzend persönlicher „smarter" Artefakte wie Kaffeetassen, Armbanduhren und Regenschirme wird es unmöglich sein, jedem Gerät einzeln die aktuellen vertrauenswürdigen Zertifikate beizubringen.

1.2.3 Transparenz

Anonymität ist nicht immer sinnvoll

Wenn Anonymität im Web bereits machbar ist – warum werden entsprechende Werkzeuge nicht einfach flächendeckend eingesetzt? Offenbar macht anonymes Surfen nicht immer Sinn: Beim Online-Einkauf beispielsweise ist die Eingabe der Lieferanschrift unumgänglich und „enttarnt" so selbst die anonymsten Besucher. Um in solchen Situationen wirkungsvoll Datenschutz gewährleisten zu können, bedarf es mehr als anonyme Kommunikationsprotokolle und sicherer (d.h. nicht abhörbarer) Datenübertragung: Es muss Benutzern möglich sein, sich bei der Herausgabe persönlicher Daten den Zweck der Erhebung, die Empfänger der Daten, die Dauer der Speicherung sowie Möglichkeiten der nachträglichen Korrektur oder Löschung klar zu machen.

P3P: ein Datenschutz-Standard für das Web

Ein erster Schritt auf dem Wege zu einer solchen Transparenz und Benutzerkontrolle im Web ist das „Platform for Privacy Preferences Project" (P3P), eine „Empfehlung" (Candidate Recommendation) des World-Wide-Web Konsortiums (W3C), welche nach mehr als dreijähriger Entwicklungszeit im Dezember 2000 veröffentlicht wurde [Lan].

Persönliche Präferenzen unterscheiden „akzeptable" von „inakzeptablen" Websites

Die Idee von P3P ist recht einfach: ein Anbieter im Web übersetzt seine Datenschutzpraktiken – d.h. eine Aufzählung der Daten, die er vom Besucher erhebt, sowie deren Empfänger, Verwendungszweck, etc. – in ein standardisiertes und maschinenlesbares XML-Format und veröffentlicht dieses auf seiner Website. Benutzer, die diese Website mittels eines P3P-fähigen Browsers besuchen, können sich die Praktiken dann komfortabel in übersichtlichen Dialogen ansehen und selbst entscheiden, ob sie unter diesen Bedingungen gewillt sind, ihre persönlichen Daten auszugeben. Haben sie einmal ihre diesbezüglichen Präferenzen in ihrem Browser eingestellt, kann dieser ihnen diese Entscheidung weiter vereinfachen, indem er au-

tomatisch Websites in „akzeptabel“ und „inakzeptabel“ einteilt. Fallen die Praktiken der Website außerhalb der Präferenzen des Benutzers, können zusätzliche Informationen und Warnungen eingeblendet werden, um eine unerwünschte Preisgabe der persönlichen Daten zu verhindern.

Detaillierte Datenschutz-Buchführung

Ob akzeptabel oder nicht – mit einem P3P-unterstützenden Browser hat der Benutzer jederzeit die Möglichkeit, die momentan gültigen Praktiken einer Website in einem relativ übersichtlichen, standardisierten Format zu inspizieren. So könnte beispielsweise beim Ausfüllen von Web-Formularen individuell der Verwendungszweck jedes einzelnen Feldes mittels eines Maus-Klicks abgefragt werden. Ebenso möglich ist eine Journal-Funktion, welche für den Benutzer über alle von ihm (bewusst oder unbewusst) ausgegebenen Daten detailliert Buch führt: wann wurde welche Information an wen zu welchen Konditionen ausgegeben, und wie kann ich meine Daten beim Service-Anbieter später ändern oder löschen?

P3P als Grundlage für Datenschutzassistenten

Auch wenn P3P in seiner ersten Version hinter den ursprünglichen Erwartungen zurück bleibt (keine digitalen Signaturen und keine abgestuften Datenschutzpraktiken für unterschiedlich personalisierte Angebote), so stellt es sicherlich einen wichtigen ersten Schritt auf dem Wege zu einem leistungsstarken Datenschutz-Assistenten dar. Es könnten hieraus auch andere Werkzeuge zur Kontrolle persönlicher Daten, auch außerhalb eines solchen Standards, hervorgehen. Sehr attraktiv ist beispielsweise die Idee eines Einzelnutzungsnachweises [Köh]: Nachdem sich Benutzer und Anbieter auf Datenschutzpraktiken verbindlich geeinigt haben, werden die erhobenen Daten bei der Speicherung direkt mit den ausgehandelten Bedingungen verknüpft. Gleich einem Einzelverbindungsnachweis beim Telefon würde anschließend jede Nutzung der Benutzerdaten vom Anbieter protokolliert und dem Eigentümer dieser Daten bei Bedarf zur Verfügung gestellt werden.

Funktioniert P3P ohne den Bildschirm?

Ob P3P als Lösung für transparente Datenschutzkontrolle im E-Commerce letztlich Fuß fassen wird, bleibt abzuwarten. Ubiquitäre Szenarien werden in jedem Fall zusätzliche Herausforderungen an derartige Mechanismen stellen: So verschwinden etwa mit der Miniaturisierung der Computer auch die im E-Commerce bisher üblichen größeren Bildschirme, auf denen eine Vielzahl von Informationen übersichtlich dargestellt werden kann. Kleinste Displays in Mobiltelefonen und Armbanduhren machen es immer schwerer, dem Benutzer solche komplexen Informationen zu vermitteln. Auch taktile Schnittstellen (z.B. Vibrations-Modus bei Handys) und Audio-Feedback eignen sich hierfür naturgemäß weniger gut.

Signalisierung des Privatsphärenzustands

Dennoch ist aber gerade in einer so umfassend überwachbaren Zukunft die einfache, verlässliche, unaufdringliche, aber doch allgegenwärtige Information über den momentanen Privatsphärenstatus unabdingbar. Während Daten, die sich nicht unterdrücken lassen (z.B. die gegenwärtige Funkzelle des Handys), rechtlich abgesichert sein müssen (d.h. keine unerlaubte Nutzung, wenn nicht durch den Benutzer oder dessen Agenten autorisiert), sollten sich alle optionalen Daten leicht durch den Benutzer bei Bedarf herausgeben lassen, ohne dass ihn eine Reizüberflutung zur unkontrollierten Ausgabe verführt (wie derzeit z.B. Cookie-Dialogboxen im Netscape Browser, die lediglich dazu führen, dass die Information vom Benutzer wieder schnellstmöglich dauerhaft ausgeblendet wird).

Delegation an Agenten

Die Delegation dieser Aufgabe an einen *Software-Agenten* ist dabei eine Möglichkeit zur komfortablen, automatischen (oder semiautomatischen) Interaktion mit Diensten in Echtzeit, die das Schnittstellenproblem mindert. Solch ein Agent würde vorher entsprechend konfiguriert und an die persönlichen Präferenzen des Benutzers angepasst, um dann in Echtzeit, ggf. abhängig vom gegenwärtigen Ort und Kontext, das Aushandeln von Datenschutzbedingungen und die eventuelle Herausgabe von persönlichen Daten zu übernehmen.

Aufklärung tut Not

Wie auch immer die technischen Lösungen in diesem Bereich ausfallen werden – eine verstärkte generelle Sensibilisierung der Benutzer ist auf jeden Fall unabdingbar. Bereits heute ist den wenigsten Internet-Nutzern bewusst, dass sie oftmals sehr persönliche Daten im Cyberspace zurücklassen. Mit dem zunehmenden „Verschwinden“ der Computer und der immer stärker werdenden „Informatisierung“ des Alltags besteht schnell die Gefahr, dass technisch unerfahrene Nutzer aus Unwissen große Teile ihrer Privatsphäre dauerhaft verlieren. Eine erhöhte Aufklärung über die Risiken dieser Technologien, z.B. in der Schule, muss sicherlich ein wichtiger Bestandteil jeder Lösung sein.

1.2.4 Vertrauen und Absicherung

EU-Datenschutz als Vorbild?

Auch wenn Gerichtsentscheide in Frankreich und Deutschland kürzlich Schlagzeilen damit machten, im bisher vielfach als rechtsfreien Raum aufgefassten Internet nationales Recht anwenden zu wollen – die Erfahrungen bisher zeigen, dass Datenschutzgesetze als nationale Insellösungen kaum Erfolg versprechen. Immerhin genießen aber EU-Bürger (und dies nicht nur beim Web-Surfen) seit In-Kraft-Treten der Direktive 95/46/EC innerhalb der Mitgliedstaaten und allen „sicheren Drittländern“ einen umfassenden Schutz vor Daten-

schutzverletzungen, der sich stark an den OECD-Richtlinien orientiert bzw. diese sinnvoll erweitert.

Safe Harbor – die amerikanische Antwort

Vor allem Artikel 25 der Direktive (Transfer personenbezogener Daten in Drittländer) hat an der momentan stattfindenden weltweiten Neuordnung nationaler Datenschutzgesetze und ihrer formellen und inhaltlichen Angleichung einen gewichtigen Anteil. Nicht zuletzt die in den USA Mitte 2000 beschlossene *Safe Harbor* Regelung birgt die Hoffnung, dass sie auf Dauer zu einer Angleichung der traditionell auf Selbstregulierung setzenden amerikanischen Praxis an europäische Standards führen wird, auch wenn die Teilnahme von US-Firmen an dem Programm noch sehr zu wünschen übrig lässt: Lediglich ein Dutzend Firmen hat sich bis Januar 2001 selbst als „sicheren Hafen" für europäische personenbezogene Daten zertifiziert [Saf].

Besonders der mangelnde Vollzug (d.h. die Überwachung und Umsetzung der Richtlinien) ist bei den Safe Harbor Prinzipien unter Kritik: Erst wenn eine Firma wiederholt durch Übertretung der Prinzipien aufgefallen ist, droht gerade einmal eine Verbannung von der Safe Harbor Liste (obwohl natürlich im US-Recht individuelle Klagen durchaus Aussicht auf Erfolg haben könnten). Während in vielen Industrienationen mehr oder weniger unabhängige Datenschutzkommissare die Einhaltung von Datenschutzgesetzen überwachen, fällt in den USA kommerziellen Gütesiegelprogrammen wie BBBOnline oder TrustE diese Aufgabe zu. Dabei verpflichten sich Firmen vertraglich, ihre Datenschutzpraktiken für den Benutzer offen zu legen und die darin gemachten Aussagen auch einzuhalten. Materielle Vorgaben zum Datenschutz, wie beispielsweise Anforderungen an die Zweckbindung oder der Vorsatz der Datensparsamkeit (d.h. nur diejenigen Informationen, die unbedingt nötig sind, werden gesammelt), sind oftmals nicht Bestandteil solcher Gütesiegel – es geht vielmehr nur darum, den Nutzer rechtzeitig zu informieren und ihm die Wahlmöglichkeit zu geben, das Angebot zu verlassen. Entsprechend erhalten auch diejenigen Anbieter ein Gütesiegel, welche offen berichten, dass sie fleißig Daten sammeln und sie an Dritte weitergeben: „Good notices of bad practices" [Roß].

Privacy Broker als Beruf?

Obwohl primär ein Konzept eines selbstregulierten Marktes, können Gütesiegelprogramme jedoch auch in Ländern mit Datenschutzkommissionen ihren Sinn darin haben, Datenschutzkommissare in ihrer Arbeit zu unterstützen und eine produktive Konkurrenz zu schaffen. Vielleicht ergibt sich sogar in Zukunft ein völlig neues Berufsbild wie etwa das des *Privacy Brokers*. Ähnlich eines Börsen-Agenten managt der Privacy Broker das Portfolio an persönlichen Benutzerdaten und setzt sich – gegen eine monatliche Grundgebühr

– für die Sicherheit und Integrität der ausgegebenen Daten ein. Vorboten solch einer Entwicklung sind die bereits in den US aufkommenden *Infomediaries*, welche aber heute eher noch im Zeichen einer Kommerzialisierung persönlicher Daten stehen: erst durch den Weiterverkauf (meist in aggregierter Form) von Benutzerdaten entsteht Profit. Umgekehrt könnte aber auch das *Privacy Management* durch vertrauenswürdige Personen oder Institutionen ein Geschäftsfeld werden – auch wenn die Vorstellung, dass umfassender Datenschutz ein Luxusgut werden könnte, das man sich erst einmal leisten können muss, etwas unbehaglich klingt.

Opt-In statt Opt-Out

In welcher Form auch immer eine rechtliche Absicherung existiert – ob staatlich reguliert oder als marktorientierte Selbstregulierung – sie muss auch ohne den expliziten individuellen Einsatz jederzeit ein Maximum an Datenschutz gewährleisten, vor allem für technisch nicht versierte Benutzer (insbesondere Kinder und Senioren). Dazu gehört beispielsweise das bewusste Entscheiden für einen Service („Opt-In“) statt das durch Voreinstellung leicht übersehbare „Opt-Out“.

Fest steht, dass in einer von allgegenwärtigen Sensoren bevölkerten ubiquitären Zukunft sowohl Opt-In als auch Opt-Out die Designer von Benutzerschnittstellen auf eine harte Probe stellen werden. Bei Opt-In-Situationen müssen für den Benutzer die Folgen klar offen gelegt werden, was besonders angesichts der oben erwähnten stark begrenzten Anzeigemöglichkeiten kreative Lösungen erfordern wird. Sollte es sich um „gepushte“ Information handeln (d.h. die Informationsübermittlung erfolgt nicht aus Eigeninitiative des Benutzers, der z.B. selbst einen Service anforderte, sondern wird unaufgefordert angeboten), muss dem Benutzer die Möglichkeit gegeben werden, zwischen interessanten und uninteressanten Angeboten automatisch unterscheiden zu können, um so Teile seiner Datenschutz-Präferenzen flexibel anzupassen.

Datenschutz-Schutzengel?

Andererseits wird es im Gegensatz zum Web in einer ubiquitären Landschaft auch eine Vielzahl von Situationen geben, in denen unweigerlich persönliche Daten durch Sensoren oder Kameras aufgenommen werden, ohne dass es eine technische Möglichkeit gibt, dieses zu unterbinden. Abgesehen von der eher unpraktikablen Vermeidung solcher Situationen (z.B. indem bestimmte Gebäude nicht betreten oder öffentliche Plätze nicht überquert werden) sollte der so überwachten Person mindestens die Tatsache der Aufzeichnung und ihr Verwendungszweck offen gelegt werden (dies könnte etwa durch ein P3P-ähnliches Protokoll geschehen), so dass sowohl in Echtzeit als auch nachträglich festgestellt werden kann, welche persönlichen Daten zu welchem Zeitpunkt wo aufgezeichnet wur-

den. Auch in diesem Zusammenhang würde der Einsatz eines Software-Agenten, der die Datenschutzpraktiken ubiquitärer Sensoren aushandeln bzw. offen legen kann, für die praktische Umsetzung geeigneter Gesetzgebungen von Bedeutung sein.

Dürfen sich Dinge an Personen erinnern?

Sicherlich wird eine praktikable gesetzliche Regelung nicht ohne substantielle technische Unterstützung auskommen, welche in geeigneten Kontexten beispielsweise Nichtabstreitbarkeit, Vertraulichkeit oder Transparenz ermöglicht. Auf der anderen Seite bleibt aber eine große Anzahl von Forderungen, welche sich nicht einfach durch technische Lösungen erfüllen lassen: Beispielsweise kann Datensparsamkeit zwar durch Technik unterstützt, nicht aber in jedem Fall erzwungen werden. Andererseits würde die Forderung nach unbedingter Zweckgebundenheit aller erhobenen Daten in einer Zukunft voll „smarter“ Kaffeetassen und mitdenkender Tische das „Gedächtnis“ solche Gegenstände geradezu verbieten – die Idee eines Gedächtnisses ist ja gerade die Speicherung von Information für zukünftige a priori unbekannte Zwecke. Da mit einer strikten Auslegung von Datenschutzgesetzen, die in einem vor-ubiquitären Zeitalter entstanden sind, viele „hübsche“ neue Anwendungen, die beispielsweise die nachträgliche Rekonstruktion des Ortsbezugs oder ein episodisches Gegenstandsgedächtnis voraussetzen, verunmöglicht würden, darf man gespannt sein, wie sich die gesellschaftliche und gesetzgeberische Diskussion hier weiterentwickelt.

1.3 Ausblick

Ronald Rivest, einer der Erfinder des RSA-Verschlüsselungsverfahrens, hat als Ursache für viele rechtliche Probleme, die wir rund um das Internet haben, einmal die „Umkehrung der Defaults“ identifiziert. Beispiele dafür sind „what was once hard to copy is now trivial to duplicate“ oder „what was once forgotten is now stored forever”, vor allem aber „what was once private is now public”. Letzteres unter anderem deswegen, weil mit dem Internet die „natürliche“ Schwierigkeit, an Information heranzukommen, wegfällt. Tatsächlich musste man früher beträchtliche Energie aufwenden, um Information zu verbreiten – heute ist es eher umgekehrt: Man muss oft einigen Aufwand treiben, um Informationen lokal oder geheim zu halten! Wenn im Zeitalter des Ubiquitous Computing das Internet bis in die Alltagsdinge hineinverlängert wird, dann wird alleine dadurch schon klar, dass hinsichtlich des Datenschutzes gewaltige Probleme auf uns zukommen könnten.

Orwells Horrorvision?

Die Vielzahl von Herausforderungen, die sich für Datenschützer und Techniker in einer Zukunft von allgegenwärtigen Computern stellen, lässt schnell die Frage aufkommen, ob es nicht unweigerlich zu den vielbeschworenen Horrorszenarien im Stile Orwells kommen wird. Für manche erscheint da die Flucht nach vorne, verbunden mit totaler Resignation, als einzige sinnvolle Alternative: „You have zero privacy anyway, get over it", wie Sun's Chairman und CEO Scott McNealy es anlässlich einer Reporterfrage auf den Punkt brachte.

Gerade die Tatsache, dass sich selbst Experten auf diesem Gebiet noch gar nicht darüber im Klaren sind, welche der vielen oft absurd klingenden Ideen – angefangen von kommunizierenden Regenschirmen, die vor einem heranziehenden Regenschauer warnen, bis hin zur „smarten" Unterwäsche, die kritische, vom individuellen Normalfall abweichende Pulsfrequenz und Atemtätigkeit dem Hausarzt weitermeldet – letztendlich eine Rolle in dieser so vagen Zukunft spielen wird, machen Voraussagen auf diesem Gebiet äußerst schwierig. Dennoch ist es sicherlich sinnvoll, die unmittelbare Zukunft – heute also vor allem die Entwicklungen im rasch wachsenden Mobilfunk-Bereich – verstärkt im Auge zu behalten, um aus dort gemachten Erfahrungen geeignete Handlungsindikatoren oder auch nur einschlägige Fragestellungen für unsere heute noch eher futuristisch anmutenden ubiquitären Landschaften zu gewinnen.

[Bäu] beschreibt angesichts der rasanten Entwicklungen in den Bereichen Internet und Mobilkommunikation vier notwendige Zutaten für „E-Privacy", einem modernen Datenschutz, der sich auch im Zeitalter von HTTP und WAP noch praktisch umsetzen lässt:

Datenschutzprinzipien für E-Privacy

- *Rechtliche Absicherung*: Ohne den Druck durch den Gesetzgeber wird es keinen wirklich wirkungsvollen Schutz geben – erst Gesetze ermöglichen eine klare Orientierung für Bürger und Wirtschaft über ihre Rechte und Pflichten.
- *Technische Unterstützung*: Ohne technische Verankerung ist Datenschutz in einer hoch technisierten Welt nicht durchführbar – Datenschützer verkommen zu Papiertigern, die undurchführbare oder unkontrollierbare Gesetze schaffen.
- *Selbstschutz*: Der Staat wird sich zwar nicht aus der Mitverantwortung stehlen können, doch wird dies in Zukunft verstärkt auch in Form von Service und Beratung für seine Bürgerinnen und Bürger geschehen müssen, damit diese informierte Entscheidungen über die Herausgabe und Verwendung ihrer Daten fällen können.

- *Marktprinzipien*: Die Datenschutzpraxis muss verstärkt darauf hinarbeiten, dass eine erhöhte Nachfrage nach Datenschutz die Produktpalette von Unternehmen ganz selbstverständlich um Angebote zum Schutz der Privatsphäre ergänzt.

Auch wenn eine „U-Privacy" auf einer Infrastruktur und einem zukünftigen Wirtschaftsgefüge aufzubauen hat, die heute kaum vorherzusagen sind, so können sicherlich einige Konsequenzen aus obigen vier Punkten abgeleitet werden:

- Die Gesetzgebung wird sich ständig an neue Realitäten anpassen müssen. Selbst weitreichend verfasste Grundsätze können kaum die technische Entwicklung der nächsten 20 Jahre berücksichtigen.
- Keine noch so umfassende technische Lösung wird Missbrauch je vollständig ausschließen können. Vielmehr ist es wichtiger, verantwortungsbewussten Datensammlern die nötigen Werkzeuge zur Verfügung zu stellen, damit der beabsichtigte Datenschutz auch umgesetzt werden kann.
- Der Einzelne muss Zugriff auf die nötigen Ressourcen haben, damit er wirkungsvollen Selbstschutz durchführen bzw. seine im Datenschutz verankerten Rechte voll wahrnehmen kann. Dass dazu auch ein gesteigertes Bewusstsein für Datenschutz notwendig ist, sollte dennoch den Uninteressierten nicht um den Mindestschutz bringen.

Handlungsspielräume?

Angesichts des rasanten technischen Fortschritts stellt sich mit Blick auf die zu erwartende Allgegenwärtigkeit des Computers und den daraus resultierenden möglichen sozialen und gesellschaftlichen Auswirkungen die Frage nach den Handlungsspielräumen. Dies ist gleichermaßen eine technische wie eine politisch-juristische Fragestellung.

In technischer Hinsicht ergeben sich oft Alternativen beim Systementwurf, oder es lassen sich von vornherein gewisse Vorgaben mit einplanen. Ein Beispiel ist die Ortslokalisierung: Im GPS-System kann ein Gerät in passiver Weise seinen Standort erfahren, ohne dass die Umgebung dies mitbekommt. Mobile Telefone dagegen sind aufgrund ihrer aktiven Kontaktaufnahme mit der nächstliegenden Funkzelle von außen innerhalb gewisser Grenzen lokalisierbar.

Wunsch und Realität

Nicht immer lassen sich jedoch an sich wünschenswerte Eigenschaften in der Praxis verwirklichen. Zum einen mögen zu hohe Kosten gegen manche Realisierungsmöglichkeiten sprechen (wenn beispielsweise jedes Kopieren und Übermitteln eines personenbezogenen Datums in nichtabstreitbarer Weise am Datum selbst

vermerkt werden soll), zum anderen lassen sich manche Aspekte aus technischen oder physikalischen Gründen kaum verwirklichen. Ein Beispiel für den zuletzt genannten Punkt wären etwa autarke Funksensoren, welche die nötige Energie zur Übermittlung des Sensorwertes über eine Distanz von einigen Metern aus dem Messvorgang selbst (etwa mittels piezoelektrischer Materialien) beziehen. Für eine sichere Verschlüsselung der Werte oder gar eine auf einem kryptographischen Challenge-Response-Protokoll basierende Authentifizierung reicht die Energie dazu im Allgemeinen nicht aus – der an sich wünschenswerten Forderung, in einer ubiquitären Welt alle Daten stets nur in gesicherter Form zu übermitteln, ließe sich also damit gar nicht nachkommen.

Was kann, was darf?

Während die Technik höchstens die Frage beantworten kann, was die Zukunft bringen *kann*, muss die Frage, was die Zukunft bringen *darf*, durch einen gesellschaftlichen Prozess beantwortet werden. Bei festzulegenden Normen und Gesetzen geht es dann darum, das Wünschenswerte mit dem Machbaren zusammenzubringen. Dies war natürlich noch nie eine einfache Angelegenheit, insbesondere wenn unterschiedliche Interessen und Wertevorstellungen mit hineinspielen, und wenn von vornherein nicht klar ist, was genau eigentlich wünschenswert ist und wo im Einzelnen die Grenzen (und Kosten) des Machbaren liegen.

Neue Spielregeln!

Wenn nun aber tatsächlich Alltagsdinge zunehmend „smart“ und vernetzt werden und sich dem Menschen gegenüber angepasst verhalten, dann führt dies letztlich zu einer anderen Welt als wir sie gewohnt sind, einer Welt in der neue Spielregeln gelten. Wie wir diese Spielregeln fassen wollen, darüber lohnt es sich jetzt schon nachzudenken.

Literaturverzeichnis

[Bäu] H. Bäumler (Hrsg.): E-Privacy, Vieweg Verlag, 2000

[Bri] D. Brin: The Transparent Society – Will Technology Force Us to Choose Between Privacy and Freedom? Perseus Press, 1999

[Gar] Simson Garfinkel: Database Nation, O'Reilly, 2000

[Han] U. Hansmann, et al: Pervasive Computing Handbook, Springer, 2001

[HUC] P. Thomas, H.W. Gellersen (Ed.): Proc. 2nd Int. Symp. Handheld and Ubiquitous Computing, Springer-Verlag, 2000

[Köh] M. Köhntopp, A. Pfitzmann: Datenschutz Next Generation, in [Bäu]

[Lan] M. Langheinrich: P3P – Ein neuer Standard für Datenschutz im Internet, digma, Zeitschrift für Datenrecht und Informationssicherheit, 2001

[Mat] F. Mattern: Das aktuelle Schlagwort – Pervasive Computing / Ubiquitous Computing, Informatik Spektrum 24/3, 2001

[Nor] D.A. Norman: The Invisible Computer, MIT Press, 1998

[Roß] A. Roßnagel: Regulierung und Selbstregulierung im Datenschutz, in: Kubicek et al. (Hrsg.): Global @home, Jahrbuch Telekommunikation und Gesellschaft, Hüthig-Verlag, 2000, pp. 385-391

[Saf] US Dept. of Commerce: Safe Harbor http://www.export.gov/safeharbor/

[Tim] D. Timmermann: Smart Environments – Technologietrends und mögliche Konsequenzen für die informationelle Selbstbestimmung, Vortrag beim Ladenburger Diskurs „Living in a Smart Environment – Implications of Ubiquitous Computing", Jan. 2001

[Wei] M. Weiser: The Computer for the 21st Century, Scientific American, September 1991, pp. 66-75