Ubiquitous Computing –
Eine Herausforderung für Datenschutz und Sicherheit

Friedemann Mattern [1]

Kurzfassung. Das noch junge Forschungsgebiet des Ubiquitous Computing beschäftigt sich damit, kleinste Computerprozessoren und mikroelektronische Sensoren in die Umwelt und in Alltagsgegenstände zu integrieren, um diese „smart" zu machen. Smarte Dinge können ihre Umgebung erfassen und dadurch Menschen bei der Bewältigung ihrer Aufgaben auf eine neue, intuitive Art unterstützen. Die Auswirkungen einer solchen umfassenden Integration von Computertechnologie in unseren Alltag sind bisher kaum abzusehen. Es ist jedenfalls mit weit reichende Konsequenzen für die Bereiche Sicherheit und Datenschutz („privacy") zu rechnen, und ohne intensive Anstrengungen auf technischer, rechtlicher oder gar politischer Ebene läuft man Gefahr, diese schöne neue Welt voller „schlauer" und kommunikationsfreudiger Dinge in einen Überwachungsstaat zu verwandeln.

1 Technologietrends

Mit der weiter zunehmenden Miniaturisierung der Computertechnologie werden in absehbarer Zukunft Prozessoren und kleinste Sensoren in immer mehr 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 oder Möbeln kommunizieren (und diese wiederum untereinander und mit den Gegenständen anderer Personen).

Schon Anfang der 1990er-Jahre hatte Mark Weiser vom Xerox-Forschungszentrum in Palo Alto diese Entwicklung vorausgesehen und in seinem einflussreichen Aufsatz „The computer for the 21st century" [9] beschrieben. Weiser prägte damals den Begriff des „Ubiquitous Computing", des allgegenwärtigen Computers, der dem Menschen unsichtbar und unaufdringlich im Hintergrund dient mit der Zielsetzung, ihn bei seinen Arbeiten und Tätigkeiten zu unterstützen und ihn von lästigen Routineaufgaben weitestgehend zu befreien.

Die treibende Kraft hinter dem stetigen technischen Fortschritt im Bereich des Ubiquitous Computing ist der langfristigen Trend der Mikroelektronik: Mit erstaunlicher Präzision und Konstanz gilt das bereits 1965 von Gordon Moore aufgestellte und nach ihm benannte „Gesetz", welches besagt, dass sich die Leistungsfähigkeit von Prozessoren etwa alle 18 Monate verdoppelt. Eine ähnlich hohe Effizienzsteigerung ist auch für einige andere Technologieparameter wie Speicherkapazität oder Kommunikationsbandbreite zu beo-

[1] ETH Zürich, Institut für Pervasive Computing

Der Beitrag basiert auf früheren Veröffentlichungen des Autors [5, 6, 7, 8] sowie der Studie „Vom Handy zum allgegenwärtigen Computer" (Verwendung mit freundlicher Genehmigung der Friedrich-Ebert-Stiftung).

bachten; umgekehrt ausgedrückt fällt mit der Zeit bei gleicher Leistungsfähigkeit der Preis für mikroelektronisch realisierte Funktionalität radikal. Dieser weiter anhaltende Trend führt dazu, dass Prozessoren und Speicherkomponenten bald noch wesentlich leistungsfähiger, kleiner und billiger werden und damit quasi im Überfluss vorhanden sein werden. Es zeichnet sich damit ab, dass unsere nahe Zukunft voll sein wird von kleinsten, spontan und drahtlos miteinander kommunizierenden Prozessoren, welche aufgrund ihrer geringen Größe und vernachlässigbaren Preises in nahezu beliebige Dinge eingebaut sein werden.

Nicht nur die Mikroelektronik trägt zur Allgegenwart und zum gleichzeitigem Verschwinden des Computers bei. Aus dem Bereich der Materialwissenschaft kommen Entwicklungen, die den Computern der Zukunft eine gänzlich andere äußere Form geben können oder sogar dafür sorgen, dass Computer auch äußerlich nicht mehr als solche wahrgenommen werden, weil sie vollständig mit der Umgebung verschmelzen. Hier wären unter anderem lichtemittierende Polymere („leuchtendes Plastik“) zu nennen, die Displays aus hochflexiblen, dünnen und biegsamen Plastikfolien ermöglichen. Laserprojektionen aus einer Brille direkt auf die Augenretina stellen eine weitere gegenwärtig untersuchte Möglichkeit zur Substitution klassischer Ausgabemedien von Computern dar. Im Bereich der Eingabemedien macht die Erkennung gesprochener Sprache langsame, aber stetige Fortschritte; schnellere Prozessoren werden die Erkennungsraten bald deutlich steigern. Es wird aber auch an „elektronischer Tinte“ und „smart paper“ gearbeitet, welche Papier und Stift zum vollwertigen, interaktiven und hoch mobilen Ein- und Ausgabemedium mit einer uns wohlvertrauten Nutzungsschnittstelle erheben. Die Bedeutung für die Praxis, wenn Papier quasi zum Computer wird oder umgekehrt der Computer sich als Papier materialisiert, kann kaum hoch genug eingeschätzt werden.

Immer wichtiger werden auch Ergebnisse der Mikrosystemtechnik und Nanotechnik. Sie führen beispielsweise zu kleinsten Sensoren, welche unterschiedlichste Parameter der Umwelt aufnehmen können. Neuere Sensoren können nicht nur auf Licht, Beschleunigung, Temperatur etc. reagieren, sondern auch Gase und Flüssigkeiten analysieren oder generell den sensorischen Input vorverarbeiten und so gewisse Muster (z.B. Fingerabdruck oder Gesichtsformen) erkennen. Eine interessante Entwicklung in dieser Hinsicht stellen Funksensoren dar, die ohne explizite Energieversorgung ihre Messwerte einige Meter weit melden können – die nötige Energie bezieht ein solcher Sensor aus seiner Umgebung oder einfach direkt aus dem Messvorgang selbst.

Ohne eigene Energieversorgung funktionieren auch die elektronischen Etiketten (so genannte „smart labels“ oder RFID-Tags). Diese sind je nach Bauform weniger als ein Quadratmillimeter groß und dünner als ein Blatt Papier. In der Form von flexiblen Selbstklebeetiketten kosten sie mit fallender Tendenz derzeit zwischen 0,1 und 1 Euro pro Stück. In gewisser Weise handelt es sich bei dieser Technik um eine Weiterentwicklung der bekannten Diebstahlsicherungen und Türschleusen von Kaufhäusern. Allerdings geht es hier nun nicht mehr nur um eine binäre Information „bezahlt / gestohlen“, sondern es

können „durch die Luft“ innerhalb von Millisekunden und bis zu einer Distanz von ca. zwei Metern einige hundert Zeichen gelesen und geschrieben werden.

Interessant an solchen fernabfragbaren elektronischen Markern ist, dass sich dadurch Objekte eindeutig identifizieren und erkennen lassen und so in Echtzeit mit einem im Internet oder einer entfernten Datenbank residierenden zugehörigen Datensatz verknüpft werden können, wodurch letztendlich beliebigen Dingen spezifische Informationen zugeordnet werden können. Lassen sich Alltagsgegenstände aus der Ferne eindeutig identifizieren und mit Information behaften, eröffnet dies aber weit über den ursprünglichen Zweck der automatisierten Lagerhaltung oder des kassenlosen Supermarktes hinausgehende Anwendungsmöglichkeiten.

Große Fortschritte werden auch auf dem Gebiet der drahtlosen Kommunikation erzielt. Interessant sind vor allem neuere Kommunikationstechniken im Nahbereich, die sehr wenig Energie benötigen und im Vergleich zu heutigen Handys kleinere und billigere Bauformen ermöglichen. Derartige Kommunikationsmodule haben derzeit etwa ein Volumen von einem Kubikzentimeter. Durch weitere Integration wird demnächst eine noch deutlich geringere Baugröße erzielt werden; der Preis liegt bei wenigen Euro und dürfte schnell weiter fallen. Ebenso intensiv wird an verbesserten Möglichkeiten zur Positionsbestimmung mobiler Objekte gearbeitet. Neben einer Erhöhung der Genauigkeit (derzeit ca. zehn Meter beim GPS-System) besteht das Ziel vor allem in einer Verkleinerung der Geräte und der Entwicklung von Techniken, die auch in geschlossenen Räumen funktionieren. Module zur Ortsbestimmung werden schon bald nur noch etwa die Größe von Kreditkarten haben.

Fasst man die genannten Techniktrends und Entwicklungen zusammen – kleinste und preiswerte Prozessoren mit integrierten Sensoren und drahtloser Kommunikationsfähigkeit, Fernidentifikation von Dingen, präzise Lokalisierung von Gegenständen, flexible Displays auf Polymerbasis, elektronisches Papier – so wird deutlich, dass damit die technischen Grundlagen für eine skurril anmutende Welt gelegt sind: Alltagsdinge, die sich aufgrund integrierter Mikroelektronik in gewisser Weise „smart“ verhalten, und mit denen wir unter Umständen sogar kommunizieren können.

Zur Realisierung einer solchen Kommunikation mit Dingen stelle man sich vor, dass Alltagsgegenstände wie Möbelstücke, verpackte Lebensmittel, Arzneimittel, Kleidungsstücke oder Spielzeug mit einem elektronischen Etikett versehen sind, das als digitale Information eine jeweils spezifische Internetadresse enthält. Kann man diese Internetadresse dann mit einem handlichen Gerät auslesen, indem man damit auf den Gegenstand zeigt, so kann dieses von sich aus, ohne weitere Zuhilfenahme des „anvisierten“ Gegenstandes, die entsprechende Information über das Mobilnetz aus dem Internet besorgen und anzeigen.

Für den Nutzer entsteht so der Eindruck, als habe ihm der Gegenstand selbst eine Information „zugefunkt“, obwohl diese tatsächlich vom Zeigegerät in indirekter Weise aus dem

Internet besorgt wurde. Bei der Information kann es sich beispielsweise um eine Gebrauchsanweisung handeln, oder um ein Kochrezept für ein Fertiggericht, oder auch um den Beipackzettel eines Arzneimittels. Was im Einzelnen angezeigt wird, mag vom „Kontext“ abhängen – also etwa davon, ob der Nutzer ein guter Kunde ist und viel für das Produkt bezahlt hat, ob er über oder unter 18 Jahre alt ist, welche Sprache er spricht, wo er sich gerade befindet – aber vielleicht ja auch davon, ob er seine Steuern brav bezahlt hat...

Bei dem Zeigegerät mag es sich in Zukunft auch um ein Stück elektronisches Papier oder um eine spezielle Brille in Kombination mit einem drahtlosen Zeigestab handeln. Außerdem sind natürlich nicht nur menschliche Nutzer an Zusatzinformation zu Gegenständen interessiert, sondern ebenso andere „schlaue“ Dinge. Eine Mülltonne mag beispielsweise sehr neugierig auf die Recyclingfähigkeit ihres Inhaltes sein, ein Arzneischrank mag um die Verträglichkeit seiner Medikamente und deren Haltbarkeit besorgt sein.

Mit der absehbaren Technikentwicklung wird somit Alltagsgegenständen eine neue, zusätzliche Qualität verliehen – diese könnten nicht nur mit Menschen und anderen smarten Gegenständen kommunizieren, sondern zum Beispiel auch erfahren, wo sie sich befinden, welche anderen Gegenstände in der Nähe sind und was in der Vergangenheit mit ihnen geschah. Dinge und Geräte können sich damit situationsangepasst verhalten und wirken auf diese Art „schlau“, ohne tatsächlich „intelligent“ zu sein.

Dadurch, dass Dinge miteinander kommunizieren können (indem diese z.B. ihren Aufenthaltsort oder Sensorwerte anderen interessierten und dazu befugten Dingen mitteilen), wird auch das Internet einen drastischen Wandel erleben. Tatsächlich ist das Wachstum des Internet ja nicht nur durch einen stürmischen verlaufenden Zuwachs hinsichtlich der angeschlossenen Computer charakterisiert, mindestens genauso interessant ist sein Wachstum in qualitativer Hinsicht: Wurde es in den 1980er-Jahren vor allem als Kommunikationsmedium von Mensch zu Mensch genutzt – E-Mail war seinerzeit die dominierende Anwendung – so brachten bereits die 1990er-Jahre mit dem WWW eine ganz andere Nutzungsform hervor: Nun kommunizierten Menschen via Browser auf der einen Seite mit Maschinen, nämlich WWW-Servern, auf der anderen Seite. Damit einher ging eine Vervielfachung des Datenverkehrs; gleichzeitig stellte dies die Voraussetzung für die schnelle Kommerzialisierung und Popularisierung des Internet dar. Jetzt zeichnet es sich indes ein weiterer Qualitätssprung ab: Das Internet wird in Zukunft vor allem für die Kommunikation von Maschine zu Maschine – oder vielleicht besser von Ding zu Ding – verwendet werden. Nachdem mittlerweile so gut wie alle Computer der Welt an das Internet angeschlossen sind, steht nun also quasi eine Verlängerung des Internet bis in die Alltagsgegenstände hinein an. Neil Gershenfeld vom Media Lab des MIT drückte dies folgendermaßen aus: „Es kommt mir so vor, als sei das rasante Wachstum des WWW nur der Zündfunke einer viel gewaltigeren Explosion gewesen. Sie wird losbrechen, sobald die Dinge das Internet nutzen“ [1].

Selbstverständlich ist die Realisierung der mit dem Ubiquitous Computing verbundenen Visionen alles andere als trivial – auch wenn man die Trends der Basistechnologien akzeptiert. Im Bereich der Informatik stellen sich beispielsweise hinsichtlich adäquater Softwarearchitekturen und einheitlicher Standards noch viele interessante Probleme. Wie lassen sich etwa die Unmengen durch smarte Dinge und Sensoren generierten Daten strukturieren, damit möglichst viele Anwendungen, die man in einer offenen Welt nicht alle kennen kann, davon profitieren können? Oder: Wie interagiert man eigentlich mit einem unsichtbaren Computer? Dies sind aktuelle Forschungsfragen, auf die wir an dieser Stelle nicht eingehen wollen – man darf in dieser Hinsicht aber sicherlich keine schnelle, umfassende Lösung erwarten.

2 Implikationen

Was bedeutet es, wenn der Computer als Gerät verschwindet, er eine Symbiose mit den Dingen der Umwelt eingeht und höchstens noch als eine Art unsichtbare Hintergrundassistenz wahrgenommen wird? Konkrete Anwendungen einzuschätzen ist schwierig, und auch Experten sind sich nicht darüber im Klaren, welche der vielen zunächst absurd klingenden Ideen – angefangen vom Fertiggericht, das Rezeptvorschläge (und Werbung) auf die Kühlschranktür projiziert, bis hin zur „smarten“ Unterwäsche, die kritische, vom individuellen Normalfall abweichende Pulsfrequenz und Atemtätigkeit dem Hausarzt weitermeldet – letztendlich eine wichtige Rolle in der Zukunft spielen könnten.

Generell scheint das Potential jedoch groß, wenn Gegenstände miteinander kooperieren können und prinzipiell Zugriff auf jegliche in Datenbanken oder im Internet gespeicherte Information haben bzw. jeden passenden Internet-basierten Service nutzen können. So gewinnt offenbar ein automatischer Rasensprenger nicht nur durch eine Vernetzung mit Feuchtigkeitssensoren im Boden an Effizienz, sondern auch durch die im Internet kostenlos erhältliche Wetterprognose. Ein anderes Beispiel sind Schreibstifte, die alles digitalisieren, was mit ihnen geschrieben wird und dies auch gleich an eine geeignete Stelle kommunizieren. Viele weitere Anwendungen „schlauer“ und kommunizierender Alltagsdinge sind denkbar. Die Grenzen liegen dabei weniger in der technischen Natur, sondern sind eher ökonomischer Art (Geschäftsmodelle, Standards, Amortisation der Infrastruktur, Kosten des Informationszugriffs etc.).

Ein hohes Anwendungspotential besitzen auch Lokalisierungstechnologien. Wird man in Zukunft kaum mehr etwas verlieren können bzw. das verlorene fast immer wieder finden, weil ein Gegenstand stets weiss, wo er ist und dies bei Bedarf mitteilen kann? Noch sind Lokalisierungsmodule, die beispielsweise auf dem GPS-System beruhen, für viele Anwendungen zu groß, zu teuer, zu ungenau und zu energiehungrig. Bei allen vier Parametern erzielt man allerdings kontinuierliche Fortschritte, und für größere und wertvolle Dinge wie beispielsweise Mietautos rechnet sich dies schon heute. Mit dem Fortschritt der Technik werden nach und nach auch einfachere Gegenstände von dieser Möglichkeit pro-

fitieren. Eltern könnten es beispielsweise zu schätzen wissen, wenn Schuhe und Jacken der Kinder ihren Aufenthaltsort verraten – die vierzehnjährige Tochter, ein auf Bewährung freigelassener Sträfling, ein untreuer Ehepartner oder der kritischer Zeitgenosse eines totalitären Regimes dürften sich darüber allerdings weniger freuen...

In gleicher Weise können „Fahrtenschreiber“ für beliebige Dinge realisiert werden: Weiss ein Gegenstand, wo er sich befindet, dann braucht er dies nur regelmäßig zusammen mit einem Zeitstempel abzuspeichern – im Nachhinein lässt sich dann die „Lebensspur“ des Gegenstandes einfach rekonstruieren und durch den Abgleich verschiedener solcher Lebensspuren kann der gemeinsame Kontext verschiedener Dinge ermittelt werden oder es kann über diese Historie einfach Zugang zu damit verbundenen Informationen (z.B. das Hotel, in dem sich eine ortsbewusste Reisetasche befand) erlangt werden.

Mittel- und langfristig dürften die diversen Techniken des Ubiquitous Computing in ihrem Zusammenspiel eine große wirtschaftliche Bedeutung erlangen. Denn werden industrielle Produkte (wie z.B. Fertiggerichte, Arzneimittel, Kleidungsstücke oder Spielzeug) durch integrierte Informationsverarbeitungsfähigkeit „schlau“ oder erhalten sie auch nur eine fernabfragbare elektronische Identität beziehungsweise Sensoren zur Wahrnehmung des Kontextes (wissen also z.B. wo und in welcher Umgebung sie sich gerade befinden), so sind dadurch innovative Produkte und ganz neue Services möglich.

In dieser Hinsicht hat die Unternehmensberatung Accenture mit den so genannten „autonomous purchasing objects“ einen schon fast provokativen Vorschlag gemacht. Dabei denkt man nicht nur an Kopierer, die in eigener Verantwortung Papier nachbestellen, sondern präsentiert dem staunenden Publikum auch Barbie-Puppen, die sich programmgesteuert und zum Entzücken der Kinder (und ihrer Eltern...) neue Kleidchen von ihrem eigenen Taschengeld kaufen: „Barbie detects the presence of clothing and compares it with her existing wardrobe. The toy can buy straight from the manufacturer via the wireless connection. She can be constantly and anonymously shopping, even though the owner might not know it“ [4].

Mit Sensoren und Kommunikationsmöglichkeiten ausgestattete Alltagsgegenstände könnten aber auch eine neue Dimension im Leasinggeschäft eröffnen. Viele Gegenstände mögen sich nämlich für das Pay-per-Use-Leasing als Alternative zum Kaufen eignen, vorausgesetzt, es kann festgestellt werden, wie oft, beziehungsweise wie intensiv, die Nutzung erfolgt – etwas, das bisher eigentlich nur beim Telefonieren, beim Stromverbrauch oder bei der Straßenmaut gut möglich war. Accenture preist dieses „continuous selling“ genannte Modell nicht nur für den Verkäufer, sondern auch für den Kunden an: „Obviously, it's great for the buyer because they only pay for what they use.“ Inwieweit die Kunden das mitmachen wollen, wird sich allerdings erst noch zeigen müssen.

Aber angenommen, ein Kurzzeitleasing ließe sich in Zukunft auf viele weitere Dinge ausweiten, für die man dann in Abhängigkeit von der tatsächlichen Nutzungsdauer be-

zahlt. Über die Zeit würden sich somit viele Kurzverträge und Micropayments summieren. Unabhängig von der technischen Realisierbarkeit drängt sich dabei die Frage auf, wie man dann noch den Überblick über die Vielzahl der abgeschlossenen Kurzzeitverträge bzw. über die unzähligen geleisteten Kleinstzahlungen behalten könnte, geschweige denn, wie sich die Rechtmäßigkeit dieser Transaktionen im Nachhinein noch überprüfen ließe. Es ist sicherlich unrealistisch, tausende von Transaktionen und Microleases von Hand nachverfolgen zu wollen, und es ist insofern fraglich, inwiefern unangemessene finanzielle Forderungen erkannt und rechtmäßige Zahlungen auch eindeutig und unabstreitbar dem Verursacher zugeordnet werden können. Es werden also sichere und gleichzeitig effiziente Mechanismen benötigt, mit deren Hilfe auch beim „ubiquitous commerce“ die Zurechenbarkeit von Forderungen und Leistungen gewahrt bleibt – möglicherweise tut sich hier auch ein Geschäftsfeld für vertrauenswürdige Intermediäre auf.

Auch wenn es im Einzelnen derzeit noch nicht abgeschätzt werden kann, dürfte jedenfalls klar sein, dass um die vielen schlauen Dinge herum völlig neue Anwendungen entstehen werden. Der digitale Mehrwert von Produkten eines Herstellers kann diese von physisch ähnlichen Erzeugnissen der Konkurrenz deutlich absetzen und Kunden stärker an eigene Mehrwertdienste und dazu kompatible Produkte binden. Die Pflege und Weiterentwicklung der für derartige Aspekte notwendigen globalen Infrastruktur – einschließlich Maßnahmen, um dem in einer solchen Umgebung erhöhten Bedürfnis nach Sicherheit und Datenschutz gerecht zu werden – mag vielleicht sogar einmal eine ganze Industrie beschäftigen, analog den heutigen Versorgungskonzernen im klassischen Telekommunikations- und Energiesektor.

Langfristig ergeben sich, bedingt durch die Anwendungsbreite des Ubiquitous Computing, viele spannenden gesellschaftliche und politische Herausforderungen. Wenn in Zukunft beispielsweise Information an „elektronisch aufgewertete“ Dinge angeheftet wird, physische Dinge also quasi selbst zu Medien werden, wer darf dann über den Inhalt bestimmen? Kann etwa eine Verbraucherschutzinstitution die in einem elektronischen Etikett eines Fertiggerichtes gespeicherte Identifikationsnummer mittels eines eigenen Verzeichnisdienstes auf eine andere Information abbilden als es der Hersteller beabsichtigt hat, um so beispielsweise vor Allergenen bei den Inhaltsstoffen warnen? Ist das zumindest dann gestattet, wenn der Nutzer dies explizit wünscht?

Viele weitere Fragen stellen sich bei der zunehmenden Informatisierung der Welt, von denen hier nur einige noch angerissen werden sollen: Funktionieren etwa viele (auch bisher eher alltägliche) Dinge nur noch dann ordnungsgemäß, wenn Zugriff auf das Internet oder eine vergleichbare Infrastruktur besteht, dann entsteht natürlich eine große Abhängigkeit von diesen Systemen und der zugrunde liegenden Technik. Wenn diese versagt, wofür es unterschiedliche Gründe – Entwurfsfehler, Materialdefekte, Sabotage, Überlastung, Naturkatastrophen, Krisensituationen etc. – geben kann, dann kann sich dies gleich in globaler Hinsicht katastrophal auswirken. Ist das korrekte Funktionieren der informati-

onstechnischen Infrastruktur überlebenswichtig für die Gesellschaft und den Einzelnen, müssen nicht nur geeignete Sicherungsmechanismen vorgesehen werden, sondern Systeme sollten von vornherein im Bewusstsein dieser Verantwortung entworfen werden.

Eine anderer Fragenkomplex betrifft die sozialverträgliche Gestaltung der skizzierten Technologien und ihrer Anwendungen. Sicherlich sollte die Nutzung der wichtigsten Funktionen einfach und allgemein möglich sein, um eine sonst tief in das alltägliche Leben hineinreichende „digitale Spaltung“ der Gesellschaft zu vermeiden. Denn da beim Ubiquitous Computing der Cyberspace mit den Dingen der realen Welt in inhärenter Weise verknüpft ist, könnte ansonsten die bei verschiedenen Bevölkerungsgruppen unterschiedlich ausgeprägte Fähigkeit, an der Informationsgesellschaft teilzunehmen, eine entsprechend reale Spaltung der Gesellschaft mit allen negativen Konsequenzen nach sich ziehen. Genauso wichtig scheint es aber auch, den Aspekt im Auge zu behalten, welche Kartelle, Monopole oder Machtkonzentrationen sich durch die Verlängerung des Internets in die Alltagswelt hinein herausbilden könnten und wie dies in einer demokratischen Gesellschaft moderiert werden kann. Vor allem aber sind den Themen „Sicherheit“ und „Schutz der Privatsphäre“ besondere Beachtung zu schenken – diesem Aspekt ist das nächste Kapitel gewidmet.

3 Herausforderungen für Privacy und Sicherheit

Schon heute sind sich nur wenige darüber im Klaren, dass beim Surfen im Internet nicht nur jeder Einkauf, sondern im Allgemeinen auch alle Mausklicks protokolliert werden und potentiell über ihre Vorlieben Auskunft geben können. Sollten sich smarte Umgebungen und schlaue Alltagsgegenstände durchsetzen, wäre mit dem Ausschalten des PCs keineswegs auch die elektronische Datensammlung beendet: Smarte Möbel und Kleidungsstücke würden fast immer aktiv sein und selbst in den eigenen vier Wänden genau wahrnehmen können, was man gerade tut, eine smarte Armbanduhr würde ständig die aktuelle Position des Benutzers ermitteln und weitermelden, um so ortsbezogene Dienste (z.B. die lokale Wettervorhersage oder die Anzeige des Rückwegs zum Hotel) nutzen zu können. Auf diese Weise entstehen, durchaus ungewollt und quasi als Nebenprodukt der Verwendung solcher bequemer oder qualitätssteigender Dienste, leicht individuelle Aktivitätsprotokolle, welche beinahe lückenlos Auskunft über das Leben einer Person geben.

Die bisher durch den Gesetzgeber erhobene Forderung nach prinzipieller Zweckgebundenheit aller gewonnenen Daten erscheint in einer Zukunft voll schlauer Küchengeräte und mitdenkender Reisetaschen nicht mehr adäquat, da sie das Gedächtnis solcher Gegenstände so gut wie verbietet – der Vorteil oder sogar die Idee eines Artefakt-Gedächtnisses liegt ja gerade in der Speicherung von Information für zukünftige aber a priori unbekannte Zwecke. Da bei einer strikten Auslegung von Datenschutzgesetzen, die in einem vor-ubiquitären Zeitalter entstanden sind, viele nette neue Anwendungen, die beispielsweise die nachträgliche Rekonstruktion des Ortsbezugs oder ein episodisches

Gegenstandsgedächtnis voraussetzen, unmöglich würden, darf man gespannt sein, wie sich die gesellschaftliche und gesetzgeberische Diskussion hier weiterentwickelt.

Neben dem Schutz persönlicher Daten zur Gewährleistung der „privacy“ ist in einem „Internet der Dinge“ natürlich auch die Datensicherheit von Bedeutung, worunter klassischerweise Vertraulichkeit, Zugriffsschutz und Authentizität fallen, aber im allgemeineren Sinne auch Eigenschaften wie Vertrauenswürdigkeit, Verfügbarkeit, Verlässlichkeit und Funktionssicherheit verstanden werden dürfen. Sicherheit ist in diesem Sinne oft auch eine Voraussetzung zur Realisierung von privacy-Schutzzielen.

In einer Welt smarter Dinge dürfte ein Hauptproblem der Sicherheit in der Heterogenität und der großen Zahl der beteiligten Komponenten liegen, die in einer offenen Umgebung sicher und verlässlich zusammenspielen sollen, wobei erschwerenderweise die Komponenten typischerweise mobil sind und untereinander spontane Kooperations- und Kommunikationsbeziehungen eingehen können. Klassische Sicherheitsprinzipien (wie z.B. Firewalls, Zertifikate, kryptographische Schlüssel), die im Allgemeinen eine eher statische Struktur und zentrale Autoritäten voraussetzen, genügen dann nicht mehr und lassen sich kaum geeignet auf die zu erwartenden Größenordnungen Dynamik hochskalieren. Die Herausforderung besteht also darin, nach Möglichkeit dezentralisierte Sicherheitsinfrastrukturen zu schaffen.

Hinsichtlich der Vertraulichkeit ist zunächst offensichtlich, dass durch die notwendigerweise drahtlose Kommunikation mobiler Gegenstände eine im Prinzip einfache Mithörmöglichkeit durch benachbarte Empfänger gegeben ist – in der Regel erscheint also eine Verschlüsselung der Kommunikation unabdingbar. Dem stehen in manchen Fällen jedoch mangelnde Ressourcen entgegen: Kleinste Sensoren etwa haben oft nur sehr wenig Energie zur Verfügung, eine Verschlüsselung der weiterzumeldenden Sensordaten kann den Energiebedarf vervielfachen, was einige Anwendungen unmöglich macht.

Weiterhin ergeben sich durch die verstärkte Mobilität von IT-Komponenten und dadurch, dass viele kleinere Alltagsgegenstände Sensoren und ein „Gedächtnis“ bekommen, neue Sicherheitsanforderungen aufgrund des möglichen Verlusts oder Dienstahls solcher Dinge: Diese könnten dann einem Fremden Aufschluss über die sehr private Lebensgeschichte des eigentlichen Besitzers geben. Ein smartes Ding darf also nur einem autorisierten Kommunikationspartner etwas mitteilen – womit sich die Frage stellt, wer in welcher Weise Autorisierungen vornehmen kann und ob sich dies weitgehend automatisieren lässt.

Offensichtlich wird man nur einer vertrauenswürdigen Instanz Zugriff auf private Daten gestatten bzw. Handlungen im eigenen Interesse ermöglichen wollen. So sollte etwa eine ortsbewusste Spielzeugpuppe für Kinder nur den Eltern (bzw. deren elektronischen Helfern) ihren Aufenthaltsort verraten, oder die Dienstwaffe eines Polizisten sollte sich nur entsichern lassen, wenn der richtige smarte Fingerring in unmittelbarer Nähe ist. Das Problem der Autorisierung ist deshalb eng verbunden mit dem Problem, die Authentizität

einer (vertrauenswürdigen) Instanz zweifelsfrei festzustellen sowie eine Art „Urvertrauen“ zu anderen Instanzen zu bekommen – ein aktuelles Forschungsgebiet.

Neben technischen Aspekten spielen bei den Themen privacy und Sicherheit auch soziale, rechtliche und politische Gesichtspunkte eine Rolle. Während man in den Anfangszeiten des Datenschutzes zunächst den allwissenden Staat beargwöhnte, inzwischen aber mehr und mehr informationshungrige Marketingabteilungen großer Firmen im Blickfeld hat, wird mit Miniaturkamera und in die Kleidung integriertem Computer jeder Einzelne zum ständigen Datensammler – oder, schlimmer noch, sogar smarte Gegenstände, für die sich niemand mehr richtig verantwortlich fühlt. An die Stelle des allwissenden „großen Bruders“ treten zahllose „kleine Geschwister“ in Form neugieriger Nachbarn und eifersüchtiger Bekannter, deren Hemmschwelle für ein gelegentliches Bespitzeln mit dem technischen Aufwand für solch eine Überwachung sinken dürfte.

In der Industrie ist man sich des ambivalenten Erscheinungsbildes des Ubiquitous Computing als eine „dual use“ Technologie durchaus bewusst. Während damit einerseits ein schon verkauftes Produkt in ein Marketinginstrument verwandelt werden kann, indem es Informationen über sich oder ähnliche Produkte anbietet und Nutzungsinformationen sammelt und dem Hersteller meldet, könnte es andererseits als Überwachungsinstrument erscheinen. In einem „white paper“ der Firma IBM [2], das die Transformation der Haushaltsgeräteindustrie zum Thema hat, wird zunächst als Vorteil für den Hersteller die Tatsache beschrieben, dass damit während der gesamten Lebenszeit eines Produktes ein Verkaufskanal zum Kunden besteht. Weiter heisst es dann aber: „A very cautious approach is needed [...] with this kind of monitoring otherwise newspaper headlines such as *'Spy in the Kitchen'* would soon appear, killing the intelligent appliance before it takes off“.

Auch im Zusammenhang mit dem seit einiger Zeit zu beobachtenden erhöhten öffentlichen Sicherheitsbedürfnis erscheint eine Entwicklung hin zum Sammeln unzähliger Daten, die isoliert betrachtet eher harmlos sind, brisant: An Stelle eines öffentlichen Aufrufs an potenzielle Zeugen nach einem Verbrechen könnte schon bald die freiwillige Freigabe der persönlichen sensorischen Datenbanken einer ganzen Bevölkerungsgruppe stehen, welche zusammen mit hoch entwickelten Suchalgorithmen eine Rasterfahndung ungeahnten Ausmaßes erlauben würde. Ähnlich den immer populärer werdenden freiwilligen DNA-Analysen würden sich bei solchen Maßnahmen all jene verdächtig machen, die den Sicherheitsorganen den uneingeschränkten Zugriff auf ihr „digitales Gedächtnis“ verweigerten.

Selbst wenn die technische Realisierbarkeit solcher Szenarien noch in ausreichender Ferne liegen sollte, so birgt deren grundlegendes Prinzip – d.h. die sekundäre Nutzung von Daten jenseits ihres ursprünglichen Zwecks – schon in näherer Zukunft Konfliktpotenzial. Nachdem Leihwagenfirmen bereits die Vorteile von GPS-Empfängern und Mobilfunk für das Lokalisieren vermisster Wagen zu schätzen gelernt haben, gibt es inzwischen erste

Verleiher, die mit der gleichen Technologie auch den pfleglichen Umgang des Mieters mit dem Fahrzeug sicherstellen: so erhebt z.B. eine Mietwagenfirma in den USA von ihren Kunden eine Gebühr für „gefährliches Fahren“, sobald sich der Wagen mit mehr als 79 Meilen pro Stunde bewegt [3]. Einige Versicherer erwägen auch bereits den Einsatz von flugzeugähnlichen „Black Boxes“ am Fahrzeug, um Kunden auf den individuellen Fahrstil optimierte Prämien berechnen zu können bzw. im Schadensfall die Schuldfrage zu klären. Schleichend entsteht so ein feinmaschiges Überwachungsnetz, welches die klassische Unschuldsvermutung der Rechtssprechung in eine grundsätzliche Schuldvermutung umkehren könnte: Wer keine eigene Aufzeichnungen des fraglichen Zeitpunktes vorweisen kann, da er bewusst auf die damit verbundenen Vorteile wie z.B. geringere Prämien verzichtet, macht sich verdächtig.

4 Fazit

Der Technologietrend zeigt eindeutig in Richtung einer weiteren Informatisierung der Welt. Die treibenden Kräfte hinter den zugrunde liegenden technischen Errungenschaften bilden die Mikroelektronik und die Informatik, unterstützt durch Grundlagenforschungen in Bereichen wie Physik und Materialwissenschaft. Die dynamische Entwicklung in diesen Gebieten geht ungebremst weiter, die Auswirkungen betreffen daher immer größere Teilbereiche des täglichen Lebens.

Der Einsatz von Ubiquitous-Computing-Systemen in der realen Welt wird langfristig positive wie negative Effekte haben, welche über die offensichtlichen, technischen Folgen weit hinaus gehen: Das politische und wirtschaftliche Machtgefüge könnte sich verschieben, neue Geschäftsmodelle dürften eine stärkere Abhängigkeit von der zugrunde liegenden Technik und damit eine höheren Anfälligkeit im Krisenfall begründen, und nicht zuletzt besteht die Gefahr, dass wir das Vertrauen in eine kaum mehr durchschaubare, allzu smarte Umgebung verlieren und so grundlegend unsere Einstellung zu der uns umgebenden Welt ändern [8]. Klar scheint jedenfalls, dass man ohne effektive Maßnahmen zum Datenschutz mit den Techniken des Ubiquitous Computing eine Überwachungsinfrastruktur schaffen würde, welche viele bestehenden Gesetze und Mechanismen zum Schutz der Privatsphäre aushebeln könnte. Es sind daher grundlegende rechtliche Überlegungen, neue technische Ansätze und auch intensive gesellschaftliche und organisatorische Anstrengungen auf den Gebieten Sicherheit und Datenschutz nötig.

In seinen Konsequenzen hinsichtlich der wirtschaftlichen Bedeutung, der Abhängigkeit von einer sicheren globalen IT-Infrastruktur und den Fragen der Sozialverträglichkeit zu Ende gedacht, dürfte die Vorstellung einer von Informationstechnik im wahrsten Sinne des Wortes durchdrungenen Welt über kurz oder lang eine gesellschaftliche und ökonomische Brisanz bekommen und so dem Ubiquitous Computing und der damit einhergehenden Ausprägung des zukünftigen „Internet der Dinge“ auch eine politische Dimension geben.

5 Literatur

[1] Neil Gershenfeld: Wenn die Dinge denken lernen. München, 1999

[2] IBM Global Services: Transforming the appliance industry – Switching on revenue streams in services. IBM White Paper, 2001.

[3] Robert Lemos: Rental-car firm exceeding the privacy limit? CNET News, Juni 2001. http://news.com.com/2100-1040-268747.html?legacy=cnet&tag=tp_pr

[4] Thomas Maeder: What Barbie Wants, Barbie Gets. Wired Magazine, 10 (1), Januar 2002.

[5] Friedemann Mattern: Ubiquitous Computing. In: H. Kubicek, G. Fuchs, D. Klumpp, A. Roßnagel (Herausgeber): Internet @ Future, Jahrbuch Telekommunikation und Gesellschaft, Band 9, p. 52-61, 2001

[6] Friedemann Mattern: Ubiquitous Computing – Szenarien einer informatisierten Welt. In: A. Zerdick, A. Picot, K. Schrape, J.-C. Burgelman, R. Silverstone (Herausgeber): E-Merging Media – Digitalisierung der Medienwirtschaft, Springer-Verlag, 2003

[7] Marc Langheinrich, Friedemann Mattern: Wenn der Computer verschwindet. Digma, 2 (3), pp. 136-140, 2002

[8] Jürgen Bohn, Vlad Coroama, Marc Langheinrich, Friedemann Mattern, Michael Rohs: Allgegenwart und Verschwinden des Computers – Leben in einer Welt smarter Alltagsdinge. In: Ralf Grötker (Herausgeber): Privat! Kontrollierte Freiheit in einer vernetzten Welt, Heise-Verlag, 2003

[9] Mark Weiser: The Computer for the 21st Century. Scientific American, 265 (9), pp. 66-75, 1991