# Datenschutz, Privatsphäre und Identität in intelligenten Umgebungen: Eine Szenarioanalyse

Michael Friedewald, Ralf Lindner
Fraunhofer-Institut für System- und Innovationsforschung, Karlsruhe

**Kurzfassung.** Der Erfolg von intelligenten Umgebungen (engl. *Ambient Intelligence*, AmI) wird entscheidend davon abhängen, wie gut persönliche Daten sowie die Privatsphäre und andere Rechte des potenziellen Nutzers geschützt werden können und ob es gelingt, Vertrauen gegenüber der wenig greifbaren informatisierten Umwelt aufzubauen. Dieser Beitrag beleuchtet diese Themen, indem Szenarien analysiert werden, die im Rahmen von technischen Entwicklungsprojekten, aber auch von politischen Entscheidungsträgern und ihren Beratern erstellt wurden. Dabei werden grundlegende Annahmen herausgearbeitet, die die Befürworter dieser Technik über den Benutzer, den Nutzungskontext und eventuell unerwünschte Nebeneffekte treffen. Auf dieser Basis wird eine Reihe von möglichen Schwachpunkten und Verwundbarkeiten intelligenter Umgebungen abgeleitet.

## Einleitung

Neben „*Ubiquitous Computing*“ und „*Pervasive Computing*“ spricht man in Europa in den letzten Jahren verstärkt von „intelligenten Umgebungen“ (*Ambient Intelligence*, AmI) [IDB01, AaM03, RFE05]. Dieser Begriff umfasst zusätzlich zur informationstechnischen Durchdringung des Alltags auch Aspekte der Mensch-Maschine-Kommunikation und der künstlichen Intelligenz. Man stellt sich dabei vor, dass eine intelligente Technik dem Menschen ständig unterstützend zur Verfügung steht, aber selbst praktisch unsichtbar wird. Dabei sollen Alltagsgegenstände zu aktiven, kommunikationsfähigen Subjekten werden und der dinglichen Welt eine ganz neue Eigenschaft verleihen: Diese wird reaktionsfähig, passt sich den aktuellen Bedürfnissen des Menschen an und steigert damit dessen Leistungsfähigkeit und Lebensqualität.

Privatsphäre, Identität, Sicherheit und Vertrauen sind in den Zukunftsvisionen über intelligente Umgebungen von Anfang an als die Schlüsselfragen schlechthin thematisiert worden [Wei93]. Innerhalb der Forschungs- und Entwicklungsszene wächst das Bewusstsein über die systemimmanente Herausforderung für soziale Normen und Werte hinsichtlich Privatsphäre und Überwachung, welche von unsichtbaren, intuitiven und allgegenwärtigen Computernetzen ausgeht.

Für die von AmI ausgehenden Gefahrenpotenziale für die Privatsphäre zeichnen zwei zentrale technische Innovationen verantwortlich: zum einen die massiv erhöhten Kapazitäten zur technischen Erfassung und Speicherung alltäglicher Aktivitäten und Interaktionen von Privatpersonen in vielfältigen Ausprägungen sowie

über große Distanzen und Zeiträume hinweg, zum anderen die gesteigerten Fähigkeiten zur schnellen Durchsuchung von großen Datenbanken, womit zusätzliche Möglichkeiten zur Erstellung von personenbezogenen Datenprofilen und anderen Formen des *Data Mining* einhergehen [BCL04]. Einer der führenden Experten auf diesem Gebiet hat folgende allgemeine Problembereiche identifiziert, mit denen die Nutzer bzw. Betroffenen von AmI sehr wahrscheinlich konfrontiert sein werden [Ack04]:

- Ein allgegenwärtiges Netzwerk von Anwendungen und Kommunikationen zieht einen massiven Anstieg bei der Erhebung und Übermittlung personenbezogenen Daten nach sich.
- Die Einführung von biometrischen Verfahren und Wahrnehmungssensoren für bestimmte Anwendungen wird die Qualität der im Umlauf befindlichen personenbezogenen Daten verändern.
- Um personalisierte Dienste anbieten zu können, wird durch AmI-Systeme ein Großteil des Alltaglebens digital erfasst (*tracking*) und gespeichert.

Freilich gilt, dass sich die angesprochenen Probleme im Bereich der Privatsphäre im Zuge der technischen Entwicklung sukzessive entfalten werden. Obwohl sich diese Zukunftsvisionen aus heutiger Warte noch weitgehend wie Science-Fiction ausnehmen, ist eine frühzeitige Auseinandersetzung mit den potenziellen Risiken der Technologie erforderlich, sollen künftige Entwicklungen in gesellschaftlich erwünschte Bahnen gelenkt werden. Um zu einem besseren Verständnis über die Funktionsweise von AmI und den inhärenten Gefahren zu gelangen, wurden über 70 F&E-Projekte und Roadmaps, die meist auch umfangreiche Szenarien enthalten, einer Metaanalyse unterzogen. Ein Großteil der untersuchten Studien wurde von der EU finanziert, etwa im Rahmen der „Disappearing Computer Initiative".

In den analysierten AmI-Visionen wird eine große Bandbreite unterschiedlicher Anwendungen angesprochen, die von vergleichsweise zeitnah zu realisierenden Prototypen bis zu Szenarien reicht, die von einem langfristigen Zeithorizont ausgehen. Die zahlreichen Facetten des künftigen Lebens in und mit intelligenten Umgebungen wurden von den Autoren in fünf unterschiedliche Hauptanwendungsbereiche gruppiert: *Zuhause*, *Arbeitsplatz*, *Gesundheitswesen*, *Shopping/Konsum* und *Mobilität*.

Nachfolgend wird der Analyserahmen vorgestellt, der die Metaanalyse der ausgewählten Studien anleitete. Von besonderem Interesse sind dabei die Untersuchungsdimensionen, anhand derer die Szenarien systematisch analysiert wurden. Die wesentlichen Ergebnisse werden dann entlang der fünf Anwendungsbereiche präsentiert, wobei die unterschiedlichen Zukunftsvorstellungen und ihre jeweiligen Besonderheiten überblicksartig diskutiert werden. Im Schlussteil geht es schließlich um die Chancen und Risiken von AmI sowie um die offenen Fragen, die sich aus den untersuchten Szenarien ergeben.

## Analytischer Rahmen

### Privatsphäre und Datenschutz

Der Schutz der Privatsphäre zählt bekanntlich zu den unverzichtbaren Vorbedingungen demokratischer Gemeinwesen. Dabei geht es nicht allein um verfassungsmäßig garantierte Abwehrrechte des Bürgers; ohne den verlässlich geschützten Bereich des Privaten sind weder die Voraussetzungen für die Pluralität politischer Anschauungen noch für öffentliche Deliberation und Meinungsbildung gegeben, auf die demokratische Prozesse angewiesen sind.

Unter Verweis auf Lessig [Les00] argumentieren Bohn et al. [BCL04], dass Individuen ihre Privatsphäre verletzt wähnen, sobald bestimmte Grenzen überschritten werden. Auf einer allgemeinen Ebene wurden folgende vier Grenzbereiche als besonders kritisch identifiziert:

- *Natürliche Grenzen*. Offensichtliche physische Grenzen wie Mauern, Türen, Kleidung, Dunkelheit, verschlossene Briefe oder Telefongespräche können als natürliche Grenzen einen Schutzraum für die wahrhaftigen Emotionen eines Menschen konstituieren.
- *Soziale Grenzen*. Erwartungen hinsichtlich der Vertraulichkeit innerhalb eines bestimmten sozialen Kontextes (z.B. Familie, Ärzte, Anwälte etc.). So besteht beispielsweise die Verhaltensnorm, dass persönlich adressierte Faxe nicht von Kollegen gelesen werden.
- *Raum- und zeitbedingte Grenzen*. In der Regel wird erwartet, dass sowohl bestimmte Lebensabschnitte als auch -bereiche isoliert voneinander bestehen können. So sollte weder eine stürmische Adoleszenzphase langfristige Auswirkungen auf das Erwachsenenleben haben, noch dürfte ein geselliger Abend mit Freunden die Zusammenarbeit im Kollegenkreis beeinflussen.
- *Grenzen aufgrund kurzlebiger oder vorübergehender Effekte*. Gemeint sind unüberlegte, spontane Äußerungen oder Handlungen, von denen der Akteur hofft, dass sie bald in Vergessenheit geraten. Ton- und Bildaufnahmen solcher Momente oder die Durchsuchung unseres Hausmülls stellen klare Verstöße gegen die Erwartung dar, dass bestimmte Informationen von Dritten unbeachtet bleiben bzw. vergessen werden.

Andere Autoren haben zur Weiterentwicklung dieser Konzeptualisierungen von Privatsphäre beigetragen. So präsentiert Nissenbaum [Nis04] ein Modell der informationellen Privatsphäre, welches auf *kontextueller Integrität* basiert. Eingriffe in die Privatsphäre sind demnach kontextabhängig: Was in einem Kontext als angemessen gilt, kann bereits in einem anderen Zusammenhang ein ungerechtfertigter Eingriff sein.

Singer [Sin01] weist darauf hin, dass das Eindringen in die Privatsphäre nicht nur Fragen der Enthüllung brisanter Informationen und die Belästigung einer Person zum falschen Zeitpunkt oder mit unerbetenen Informationen betrifft. Personalisierung von Information könne durchaus im Interesse des Betroffenen sein, wenn dies beispielsweise die Zahl unerwünschter und lästiger Werbung reduziert. Aller-

dings könnten die denkbaren Vorteile der Personalisierung gerade mittel- und langfristig besonders negative Konsequenzen zeitigen, da durch die Reduzierung des Individuums auf eine schlichte Konsumentenrolle die Fähigkeiten des Abwägens und des reflektierten Handelns nicht gefordert werden.

## Methodik der Szenarioanalyse

Die Entwicklung von Szenarien ist eine sinnvolle Methode, um die prominentesten Forschungs- und Entwicklungsaktivitäten innerhalb eines bestimmten Technologiebereichs in einer konzisen Form zu präsentieren. Mit Blick auf die Szenarien im Bereich von AmI lassen sich mindestens drei Typen unterscheiden:

- Elaborierte Szenarien (*screenplays*) beinhalten sehr detaillierte Angaben zu Akteuren und ihren Aktivitäten und basieren auf einem sorgfältig ausgearbeiteten Handlungsstrang. Diese Szenarien können entweder primär konzeptionelle, hypothetische Visionen über eine Zukunft sein,[1] oder der Darstellung von Zielen innerhalb eines Projektes dienen.
- Anwendungsszenarien finden sich meist in Forschungsveröffentlichungen. Hierbei konzentriert man sich auf eine bestimmte Funktion des in den Publikationen behandelten Prototyps; die Handlungsstränge sind nur dort ausgearbeitet, wo dies der Darstellung und Problematisierung der unmittelbaren Funktionalität des Prototyps dienlich ist.
- Der am weitesten verbreitete Typus ist streng betrachtet kein Szenario im eigentlichen Sinne. Diese „Szenarien“ basieren nicht auf stimmigen Geschichten, sondern beschreiben bestimmte Situationen und/oder Trends, die sich für die Anwendung von AmI-Technologie besonders gut eignen könnten.[2] Solche Darstellungen verweisen oft auf interessante Anwendungsgebiete, die meist weder in den Szenarien des ausführlicheren ersten noch des technikorientierten zweiten Typs auftauchen.

Die ausgewählten Zukunftsvisionen und Szenarien wurden entlang folgender Dimensionen systematisch analysiert:

- Charakteristika des *Hauptakteurs*. Fragen der Privatsphäre sind abhängig vom eigentlichen Darstellungsziel des Szenarios. So ist es etwa denkbar, dass Menschen mit Behinderungen eine größere Bereitschaft haben könnten, private Informationen gegen bestimmte Formen der alltäglichen Unterstützung einzutauschen als Nicht-Behinderte. Auch die Lebensphase eines Menschen spielt eine entscheidende Rolle, da beispielsweise davon auszugehen ist, dass kleine Kinder ein weniger ausgebildetes Interesse am Schutz ihrer Privatsphäre haben.

[1] Ein gutes Beispiel stellen etwa die Szenarien der *Information Society Technologies Advisory Group* (ISTAG) dar [IDB01].

[2] Siehe beispielsweise [MMS03] zur Rolle von Technologie bei der Rettung von Lawinenopfern.

- *Kontext* des Szenarios. Menschen haben unterschiedliche Erwartungen hinsichtlich des Schutzes der Privatsphäre in Abhängigkeit von der jeweiligen Umwelt. So gelten in der Öffentlichkeit allgemein anerkannte Verhaltensrestriktionen, die in dieser Form innerhalb der Privatwohnung kaum akzeptiert werden würden.
- *Handlungen* innerhalb des Szenarios. Die im Szenario beschriebenen Aktivitäten des Akteurs sind ein konstituierender Teil sowohl des Handlungsstrangs als auch des persönlichen Kontextes des Akteurs.
- *Informationsflüsse* innerhalb des Szenarios. Übermittlung und Austausch von Informationen sind deshalb von herausragender Bedeutung, weil mit ihnen Gefahren der (unfreiwilligen) Offenlegung verbunden sind.
- Der *Grad der Kontrolle* des AmI-Systems. Mit dem Ausmaß der vom AmI-System ausgeübten Kontrolle gehen Fragen der Abhängigkeit von der Technologie, der rechtlichen Verantwortung für eigenständige Aktionen des technischen Systems und, mit diesen beiden Aspekten eng verknüpft, der gesellschaftlichen Akzeptanz einher.
- *Implementierung* von AmI-Systemen. Viele Gefahren für eine unversehrte Privatsphäre gehen vom eigentlichen Prozess der praktischen Umsetzung technischer Systeme aus.

## Zukunftsvisionen

Bevor die Kernfragen von Privatsphäre, Identität und Datensicherheit erörtert werden, werden nachfolgend zunächst die Hauptanwendungsbereiche von AmI-Systemen (Privathaushalt, Arbeitsplatz, Gesundheitswesen, Shopping/Konsum und Mobilität) auf einer allgemeinen Ebene vorgestellt.

### Privathaushalte

Die Wohnung, das Zuhause, ist bekanntlich der Ort für Privatheit schlechthin. Die private Umgebung und die dortige Atmosphäre haben einen entscheidenden Anteil am persönlichen Wohlbefinden. Möchte man sensible private Informationen über eine Person in die Hände bekommen, ist die Privatwohnung sicherlich der am besten geeignete Ort für entsprechende Auskundschaftungen. Innerhalb der Privatwohnung werden persönliche und finanzielle Dinge besprochen und erledigt; individuelle Verletzbarkeiten, Schwächen und Gesundheitsprobleme werden dort am ehesten offenbart. Es existieren nur wenige persönliche Informationen über Individuen, die nicht in einer Privatwohnung aufgefunden werden könnten. Aus der Perspektive des Individuums wird das Zuhause als jener Ort wahrgenommen, wo er sich ohne äußere Eingriffe weitgehend frei entfalten kann. Nissenbaum [Nis04] betont, dass insbesondere dieser Aspekt von Privatheit für die Persönlichkeitsentwicklung und -entfaltung von großer Bedeutung ist.

Ein großer Teil der AmI-Projekte und der Roadmap bzw. Szenarien setzt sich mit dem Zuhause auseinander [FDP05]. Dabei spielen insbesondere folgende Themen und Anwendungsmöglichkeiten eine Rolle:

- Individuelle Kommunikationsangebote sowohl für die Kommunikation unter den Haushaltsmitgliedern als auch zwischen Personen innerhalb und außerhalb der Wohnung. Die Kommunikationsanwendungen, die in den Visionen über die Haushalte der Zukunft thematisiert werden, zielen meist auf den Aufbau von Informationsaustausch zwischen Freunden und Familienmitgliedern ab, womit die Übermittlung großer persönlicher Datenmengen verbunden ist [AHC01, IDB01, MYA05, MaB03].
- Personalisierter Zugang zu externen Informationsangeboten.
- Technische Unterstützung bei der Suche nach persönlichen Gegenständen (Spielzeug, Schlüssel etc.) [ORB99, AHC01].
- Bedienung und Kontrolle von Haushaltsgeräten aller Art, um Reproduktionsarbeiten zu unterstützen [AHC01, MaB03].
- Erhöhung von Sicherheit durch die technisch unterstützte Nachverfolgung (*tracking*) von Personen, Geräten und Objekten; Unfallvorbeugung und schnelle, automatisierte Übermittlung von Notfallmeldungen; Zugangskontrollmanagement [AHC01, ITE04].
- Freizeit- und Unterhaltungsangebote sowie Verbesserung des alltäglichen Komforts [AHC01, PTA01, ITE04].

Die Mehrzahl der untersuchten Szenarien im Bereich des Anwendungsgebiets Privathaushalt macht keine näheren Angaben zur konkreten Lage der Wohnungen, d.h., es bleibt unbestimmt, ob es sich um eher ländliche oder städtische Gebiete handelt. Daraus ist zu schließen, dass das Zuhause der Zukunft als ein komplexes System angesehen wird, das von einer Infrastruktur unterstützt wird, die grundsätzlich universell zur Verfügung steht. Ferner wird die Wohnung als Privatsphäre konzipiert, die jedoch halb-öffentlich werden kann, sobald Besucher eintreten.

### Arbeitsplatz

Für den AmI-Anwendungsbereich „Erwerbsarbeit“ sind drei Aspekte von besonderer Bedeutung: (1) Zwar verbringen Menschen in der Regel einen hohen Anteil ihrer Lebenszeit am Arbeitsplatz, allerdings sind sie dort im Vergleich zu ihrem Zuhause weitaus weniger in der Lage, ihre Umweltbedingungen selbst zu bestimmen. (2) Sollten Arbeitgeber die Privatsphäre ihrer Mitarbeiter beeinträchtigen, bleibt den abhängig Beschäftigten aufgrund der strukturellen Asymmetrie der Beziehung meist nur die Möglichkeit, die Situation zu akzeptieren oder den Arbeitgeber zu wechseln. (3) Unabhängig davon ist es wahrscheinlich, dass Arbeitnehmer unter als ungerechtfertigt wahrgenommenen Eingriffen in ihre Privatsphäre leiden. Dabei bleibt die Frage offen, ob und in welchem Ausmaß ein Arbeitgeber von einer intensiven technischen Überwachung seiner Beschäftigten profitiert oder aufgrund von Leistungsverlusten mehr Nachteile erleidet.

Die Grenzziehung zwischen Privat- und Arbeitsphäre bleibt dennoch unscharf. So lässt es sich aufgrund der üblichen Arbeitszeiten kaum vermeiden, dass auch am Arbeitsplatz private Dinge erledigt werden. Daraus folgt, dass mit Blick auf das Arbeitsumfeld nicht nur rechtliche Fragen des Urheberrechts u.Ä. von Bedeutung sind, sondern eben auch der Schutz privater Daten.

Die Analyse der auf den Arbeitsbereich zielenden AmI-Forschungsprojekte verdeutlicht, dass AmI-Systeme bereits heute an manchen Arbeitsplätzen aufgebaut werden. Daher liegt der Schluss nahe, dass wir weitaus schneller mit intelligenten Umgebungen am Arbeitsplatz konfrontiert sein werden, als dies in Privathaushalten der Fall sein wird. Dem Schutz der Privatsphäre in der Arbeit kommt somit zumindest kurzfristig eine höhere Dringlichkeit zu.

AmI-Projekte und Roadmaps bzw. Szenarien im Anwendungsbereich Arbeitsplatz setzen sich wie folgt mit diesem Themenkreis auseinander [AsH02, Lop04, LHN04, Hei04]:

- Individuelle Kommunikationsangebote, sowohl für den Informationsaustausch unter den Mitarbeitern als auch zwischen den Personen innerhalb und außerhalb des Arbeitsbereichs. Dabei wird sowohl die dienstliche als auch die private Kommunikation behandelt.
- Unterstützung der Mobilität von Mitarbeitern, um prinzipiell zu jeder Zeit und an jedem Ort die Arbeitsaufgaben durchführen zu können.
- Zugang zu arbeitsrelevanten Informationen zu jeder Zeit und an jedem Ort, um *knowledge-sharing* und Kooperation zu verbessern.
- Schaffung eines Angebots an effizienten Unterstützungswerkzeugen, beispielsweise leistungsfähige Tools für das Dokumentenmanagement, Unterstützung von Besprechungen durch Multimedia-Anwendungen etc.
- Bedienung und Kontrolle von Arbeitsgeräten wie Projektoren oder Bildschirmen. Durch die Verknüpfung unterschiedlicher Applikationen können ganze Gebäude zu intelligenten Umgebungen werden, wodurch beispielsweise die Aufenthaltsorte der Mitarbeiter lückenlos nachvollzogen und sie jederzeit kontaktiert werden können.
- Erhöhung des Sicherheitsniveaus in Abhängigkeit der jeweiligen Arbeitserfordernisse.
- Arbeitsgebietsspezifische Funktionalitäten wie Diagnoseinstrumente, Produktionsautomation, Lagerhaltung oder dynamisches Preismanagement.

Ähnlich wie für den Bereich der Anwendungen für zu Hause, wird auch für das Arbeitsumfeld angenommen, dass die notwendige Infrastruktur für AmI-Systeme grundsätzlich überall vorhanden ist. Durch die allgegenwärtige Existenz von Kommunikationsgelegenheiten sind Mitarbeiter überall und zu jeder Zeit erreichbar, während diese umgekehrt stets Zugriff auf die Daten ihres Aufgabenbereichs haben. Zwar gilt der Arbeitsplatz generell als ein halb-öffentlicher Ort, dennoch nehmen die meisten Beschäftigten ihr unmittelbares Umfeld (Büro, Schreibtisch etc.) als ihren zumindest in Teilen privaten Bereich wahr, der weniger Verhaltensrestriktionen unterliegt als vollständig öffentliche Orte.

## Gesundheit und Pflege

Für den Anwendungsbereich Gesundheit und Pflege sind zwei Aspekte prägend, die zueinander in einem Spannungsverhältnis stehen: Einerseits hat das Gesundheitssystem großen Einfluss auf Lebensqualität und Lebenserwartung; zudem kann der schnelle Zugriff auf individuelle Gesundheitsinformationen (z.B. Allergien, Krankheitsgeschichte etc.) gerade in Notfällen lebensrettend sein. Andererseits zählen persönliche Gesundheitsinformationen zu den sensibelsten Informationen schlechthin. Bei vielen Menschen besteht nur eine sehr geringe Bereitschaft, Informationen über ihre Gesundheitssituation selbst gegenüber engen Verwandten preiszugeben. Dies gilt erst recht und umso mehr gegenüber neugierigen Vorgesetzten und Versicherungsunternehmen. Vor diesem Hintergrund besteht die Herausforderung für das Design von AmI-Systemen im Gesundheitswesen darin, Rettungskräften und Ärzten den erforderlichen Informationszugang zu ermöglichen, während zugleich allen anderen Personengruppen dies ohne ausdrückliche Zustimmung des Betroffenen verwehrt bleiben muss [Cas04].

Die wichtigsten AmI-Anwendungen im Bereich Gesundheit und Pflege sind:

- *Prävention*. Der Bereich Vorsorge und Prävention umfasst die kontinuierliche technische Überwachung des Gesundheitszustands sowie des gesundheitsrelevanten Verhaltens (Ernährung, Sport etc.); die Förderung von gesunden Verhaltensweisen und andere Beratungsdienstleistungen; Warnungen vor ungesunder und/oder gefährlicher Nahrung (etwa bei Allergien) sowie Prognosen über künftige Gesundheitsrisiken (z.B. mit Hilfe von Genanalysen) [SLK01, ITE04, Riv03, CaR05].
- *Heilung*, insbesondere die kurzfristige Genesung. Heilung in den AmI-Szenarien umfasst eine breite Palette, die von der Diagnose bis zur eigentlichen Behandlung zu jeder Zeit und an jedem Ort reichen kann. Dies wird etwa durch den Aufbau von Ad-hoc-Netzen für den Informationsaustausch zwischen medizinischem Personal erreicht. Zudem können mikroskopisch kleine AmI-Anwendungen die Medikamentenverabreichung übernehmen (etwa in Gestalt von Implantaten). Auch für die automatisierte und kontinuierliche Überwachung bei chronischen Erkrankungen können AmI-Systeme sinnvoll zum Einsatz kommen, indem sie im Falle einer Krise die notwendigen Medikamente verabreichen [Riv03, SLK01, JDS04, VLN04].
- *Pflege*, ausgerichtet auf die Rekonvaleszenz von Patienten sowie auf die Unterstützung von alltäglichen Verrichtungen von Personen, die langfristig oder dauerhaft auf die Hilfe Dritter angewiesen sind. Dies kann auch eine Rund-um-die-Uhr-Überwachung implizieren, um ein möglichst selbstständiges und unabhängiges Leben während der Pflegephase zu ermöglichen. Zu den Mitteln, um dieses Ziel zu erreichen, zählen (1) AmI-Systeme, die in der Lage sind, die Aktivitäten des Patienten zu erfassen, mögliche Anomalien zu identifizieren und gegebenenfalls Ratschläge in einer angemessenen Form zu erteilen, sowie (2) technische Hilfsmittel wie Hörgeräte, Prothesen oder Implantate (z.B. Herzschrittmacher) [MoR05, CaR05, Riv03].

- *Verbesserung der Informationskette* in Notfällen, wobei dies von der Übermittlung von Notrufen bis zur Vorbereitung erster Behandlungsschritte reichen kann [SLK01].

### Shopping und Konsum

AmI-Applikationen im Anwendungsbereich Einzelhandel und Shopping zielen auf die Schaffung von nutzerfreundlichen, effizienten und allgegenwärtigen Diensten ab. Diese Systeme können dazu beitragen, den Konsumenten bei der Suche und Auswahl von Gütern und Dienstleistungen zu unterstützen und die Prozesse der Bestellung, Bezahlung und Zustellung der gekauften Waren effizienter zu gestalten.

Eine kommerzielle Transaktion besteht aus einem komplexen Bündel unterschiedlicher Handlungen, beginnt mit dem Betreten des Geschäfts, umfasst die Auswahl des Produkts, den Kauf und schließlich die Bezahlung und zieht gegebenenfalls die Zustellung und den Umtausch der Ware nach sich. Die wichtigsten AmI-Dienste für den Konsumenten, die in den Szenarien behandelt werden, sind:

- *Persönliche Einkaufsmanagement-Systeme*. Sie unterstützen den Verbraucher bei der Erstellung von Einkaufslisten, indem der Bestand von Nahrungsmitteln und anderen Gebrauchsgütern überwacht und intelligent mit den Konsumpräferenzen und Gewohnheiten des Nutzers in Beziehung gesetzt werden. Dazu ist wiederum die Erstellung eines persönlichen Profils des Konsumenten erforderlich [AHC01, IDB01].
- *AmI-fähige Geschäfte (smart shops)*. Diese ermöglichen es Kunden, Waren mit Hilfe von Produkt-*Tags* und intelligenten Hilfsmitteln wie Einkaufswagen, mobilen persönlichen Assistenten (PDA) etc. gezielter ausfindig zu machen und schließlich leichter zu erwerben. Intelligente Kassensysteme, Wunschlisten sowie Daten über das Einkaufsverhalten eröffnen dem Geschäftsinhaber erweiterte Möglichkeiten zur Umsatzsteigerung [Har05].
- *Bestell- und Bezahlsysteme*. Diese können so unterschiedliche Funktionen wie eine digitale Kundenkartei oder das Management von Rabattmarken, Sonderangeboten, Lagerbestand und Warenauslieferung beinhalten [IDB01].

Ganz ähnlich wie in anderen AmI-Anwendungsbereichen auch wird das Einkaufen überwiegend als eine Tätigkeit dargestellt, die weitgehend unabhängig von Raum und Zeit durchgeführt werden kann. Die Szenarien, in denen das Einkaufen als Aktivität beschrieben wird, in der der Kunde physisch anwesend ist, machen indes keine näheren Angaben zur Lage der Geschäfte. Damit wird impliziert, dass AmI-fähige Geschäfte flächendeckend verbreitet sein werden. In den Szenarien, in denen Bestell- und Liefersysteme thematisiert werden, wird stillschweigend die Existenz einer angemessenen Auslieferungslogistik vorausgesetzt. Ohne dass dies in den Texten explizit gemacht wird, werden sich solche Infrastrukturen vermutlich zunächst in dichter besiedelten Regionen herausbilden.

### Mobilität

Die *ITEA Technology Roadmap on Software Intensive Systems* [ITE04] thematisiert „*nomadic applications*“, welche dieselben Funktionalitäten und Dienste wie in den Anwendungsbereichen „Zuhause“ und „Arbeitsplatz“ zur Verfügung stellen. Im Gegensatz zu den ortsgebundenen Anwendungen kann der Nutzer von diesen Diensten jedoch von unterschiedlichen Standorten aus und/oder während des Ortswechsels Gebrauch machen.

Für mobile AmI-Systeme sind zwei Eigenschaften von besonderer Bedeutung: Erstens sind mobile Nutzer nicht in der Lage, die jeweilige Umgebung, in der sie sich zeitweise befinden, zu kontrollieren. Zweitens ist davon auszugehen, dass Reiseaktivitäten sowohl dienstlichen als auch privaten Zielen dienen. Daraus folgt, dass der Schutz privater Daten auch und insbesondere im Bereich der mobilen Anwendungen sichergestellt werden muss. Ansonsten werden Reisende entweder die inhärenten Risiken für ihre Datensicherheit hinnehmen müssen oder aber ihre Mobilität einschränken. Letzteres ist insbesondere für dienstlich motivierte Ortswechsel schlicht nicht praktikabel.

AmI-Systeme sind bereits heute auf dem Vormarsch, etwa in Gestalt der biometrischen Reisepässe, die in den kommenden Jahren in den meisten EU-Mitgliedsstaaten verpflichtend eingeführt werden. In den untersuchten Szenarien stehen folgende AmI-Dienste für den Anwendungsbereich Mobilität im Mittelpunkt:

- Zahlreiche Kommunikationsformen, beispielsweise zwischen Familienmitgliedern, die sich an unterschiedlichen Orten befinden, oder zwischen Fremden innerhalb eines Aufenthaltsortes. Im Gegensatz zum Anwendungsbereich „Zuhause“ kann Video-Kommunikation zwischen Eltern und ihren Kindern von beiden autonom initiiert werden. Typische Formen des Informationsaustauschs in Mobilitätsszenarien sind Tele-Verbindungen zu Daten und Personen zu Hause, an den Arbeitsplatz und zu Freunden und Familie.
- Eine Kommunikationsform, die besondere Aufmerksamkeit verdient, sind die so genannten *negotiation tools*. Diese Applikationen ermöglichen „Verhandlungen“ zwischen unterschiedlichen Agenten (PDAs, Transaktionsagenten etc.). In den Mobilitätsszenarien spielen *negotiation tools* eine herausragende Rolle, da sie bestimmte Aktivitäten wie die Passkontrolle am Flughafen „im Vorübergehen“ erledigen können [LMP03].
- Umfassender Informationszugang (privat, dienstlich, Gesundheit, Unterhaltung etc.).
- Effiziente AmI-Transportsysteme (z.B. verlässliche, personalisierte Verkehrsinformationen in Echtzeit).
- Sicherheit, etwa im Straßenverkehr durch automatisierte Überwachung des Autofahrers oder durch die automatische Registrierung von Störungen.
- Effiziente Bezahlsysteme, etwa für Mautstraßen, Eintrittskarten und andere gebührenpflichtige Angebote.
- Unterstützung in Notfällen, z.B. durch die schnelle Identifizierung von Verletzten und die rasche Informationsweitergabe an die zuständigen Stellen.

- Zugangskontrollen, von Mietwagen bis zu Grenzübergängen. In diesen Bereich fällt auch die Kontrolle über die Information, ob eine Person erreichbar ist oder nicht.

Obwohl sich die in den Mobilitätsszenarien behandelten AmI-Funktionen nur unwesentlich von jenen der Anwendungsbereiche „Zuhause" und „Arbeitsplatz" unterscheiden, sind die jeweiligen Anforderungen an AmI-Systeme für Mobilität sehr unterschiedlich, je nachdem ob die Dienste von einem festen Ort aus oder während der eigentlichen Reiseaktivität genutzt werden. Die Grenzen zwischen privaten und öffentlichen Kontexten sind grundsätzlich ausgesprochen unscharf, und Nutzer können rasch und mit hoher Frequenz zwischen den unterschiedlichen Sphären wechseln.

## Ergebnisse der Szenarioanalyse

In den vorangegangenen Abschnitten wurden Funktionen und Kontextbedingungen von AmI-Systemen in unterschiedlichen Anwendungsbereichen dargestellt. Im Folgenden geht es um die potenziellen Gefahren für die Privatsphäre sowie um die gesellschaftlichen Implikationen, die von der Technologie unabhängig vom konkreten Anwendungsbereich ausgehen.

### Die typischen Nutzer

Die Mehrzahl der analysierten Szenarien handelt von Arbeitnehmern. Ferner wird angenommen, dass die meisten Menschen, einschließlich der Senioren, AmI-Technologie bereitwillig angenommen haben. Mit Ausnahme jener Szenarien, die sich mit der Unterstützung von Einkäufen und anderen alltäglichen Verrichtungen älterer, in aller Regel alleinstehender Menschen befassen, werden die gewöhnlichen Tätigkeiten wie Einkaufen, Fernsehen usw. überwiegend am Beispiel eines gesunden, relativ wohlhabenden Erwachsenen dargestellt.

Allerdings können AmI-Systeme, die den Anwender primär als Individuum konzeptualisieren, mit problematischen Nebenwirkungen für soziale Beziehungen, etwa innerhalb von Familienverbänden, verbunden sein. In diesem Zusammenhang sei auf die Szenarien verwiesen, die beschreiben, wie AmI-Fernseher auf der Grundlage von physiologischen Signalen den Nutzer bei der Auswahl des gewünschten TV-Programms unterstützen. Dabei bleibt fast immer unerwähnt, dass ein Haushalt aus mehreren Personen mit nicht immer deckungsgleichen Interessen bestehen kann. Hinsichtlich der Möglichkeit gegenläufiger Interessen ist das ITEA-Szenario „*The Rousseaus' Holiday*" eines der wenigen Ausnahmen [ITE04, 134ff.]. In jenen Fällen, in denen der Anwender beispielsweise durch beschwingte Musik geweckt wird, wird entweder unterstellt, er sei allein im Schlafzimmer, oder aber alle Haushaltsmitglieder stünden zur selben Zeit auf und hätten zudem einen sehr ähnlichen Musikgeschmack [SLK01]. Ganz ähnlich verhält es sich mit

Shopping-Szenarien, die häufig vernachlässigen, dass Einkaufen nicht zwingend eine individuelle Tätigkeit, sondern in vielen Fällen in einen gemeinschaftlichen Zusammenhang eingebettet ist, in welchem die einzelnen Haushaltsmitglieder unterschiedliche Verantwortlichkeiten und Kompetenzen innehaben. So wird nur selten berücksichtigt, dass Kinder zwar durchaus bestimmte Dinge auf eine Einkaufsliste setzen dürfen, zugleich aber Eltern das Recht haben, solche Entscheidungen rückgängig zu machen [AHC01]. Minderjährige werden im Großteil der Szenarien ohnehin nur selten als Menschen mit eigenständiger Persönlichkeit und bestimmten Verantwortungsbereichen portraitiert. Die Rollen, die ihnen zugewiesen werden, beschränken sich meist auf die des Nutzers von Spielen, des Objekts der Überwachung durch die Eltern oder des Empfängers von automatisierten Erinnerungen, bestimmte Dinge zu erledigen.

Besondere Aufmerksamkeit wird der verbesserten interpersonalen Kommunikation gewidmet. Kommunikation zwischen Familienmitgliedern, Freunden, Kollegen aber auch zwischen Unbekannten wird asynchron, synchron, zu Hause, am Arbeitsplatz oder unterwegs ermöglicht. Ein Sonderfall stellt die Kommunikationssituation zwischen Eltern und ihren Kindern dar, die in vielen Szenarien so konfiguriert ist, dass Erwachsene die Kommunikationsverbindung initiieren, um zu kontrollieren, was die Sprösslinge gerade tun. Dabei bleibt die Frage unbeantwortet, ob und gegebenenfalls unter welchen Bedingungen die Minderjährigen das Recht haben, sich der jederzeit möglichen Observation zu entziehen. Die Kinder stellen in den Szenarien hingegen Kommunikationsverbindungen meist dann her, wenn ihre Eltern auf Reisen sind. Insgesamt wird die bedeutende Rolle vernachlässigt, die junge Menschen bei der Aneignung und Diffusion neuer Kommunikationstechnologien und -dienstleistungen (z.B. SMS, Klingeltöne etc.) seit langem spielen.

Die Szenarien im Gesundheitsbereich unterscheiden sich von den übrigen Anwendungsbereichen vor allem dahingehend, dass es sich bei den Hauptakteuren um Senioren, Personen mit Behinderungen, chronischen Krankheiten oder besonderen Gesundheitsrisiken handelt. In den meisten Beispielen werden die gesundheitlichen Beeinträchtigungen so dargestellt, als läge in der AmI-Technologie die einzige Möglichkeit zur Verbesserung der Lebensumstände. In der Regel wird impliziert, dass die AmI-Systeme ausgezeichnet funktionieren und für die Anwender keinerlei Schwierigkeiten erzeugen.

In Szenarien wird häufig auch unterstellt, dass die intelligenten Umgebungen – seien es *smart shops* oder ganze Städte – nicht nur von allen akzeptiert, sondern auch für alle bezahlbar sind.

### Kontrolle über den Anwender

Umfang und Intensität der Kontrollmöglichkeiten, die AmI-Systeme über den Anwender ausüben, variieren erheblich in Abhängigkeit von der jeweiligen Applikation. So üben AmI-Systeme einen hohen Grad der Kontrolle aus, wenn sie stellvertretend für eine Person aktiv werden, etwa wenn das System ankommende Anrufe verwaltet oder aber eigenständig persönliche Daten weiterleitet. Ein

mittleres Kontrollniveau wird erreicht, wenn sich AmI-Systeme auf informierende bzw. beratende Funktionen beschränken, z.B. Vorschläge über das angemessene Verhalten im Straßenverkehr erteilen. Ein niedriges Kontrollniveau wird schließlich erreicht, wenn AmI-Systeme ausschließlich Befehle der Anwender ausführen.

In den meisten Szenarien der unmittelbaren und in nahezu allen Szenarien über die fernere Zukunft haben AmI-Systeme ein hohes Kontrollniveau inne mit Blick auf Schutz und Sicherheit (etwa in Gestalt von Zugangskontrollen zu Online-Diensten, Wohnungen, Autos, Arbeitsstätten, Krankheitsdaten, finanziellen Transaktionen oder grenzüberschreitendem Verkehr) sowie hinsichtlich des Schutzes der Privatsphäre. Letzteres folgt aus dem Umstand, dass in den Szenarien keine Situationen portraitiert werden, in denen ein Anwender Zugang zu und Kontrolle über persönliche Daten erhält; damit wird impliziert, dass AmI-Systeme umfassende Kontrolle in Fragen des Schutzes der Privatsphäre ausüben.

Ein hoher Kontrollgrad ist ferner mit jenen AmI-Anwendungen verbunden, die lebenserhaltende bzw. -sichernde Funktionen ausüben. Dazu zählen die Bereiche der permanenten Überwachung des Gesundheitszustands sowie die Erkennung akuter Krisen (z.B. eines Herzinfarkts) und der sicheren Mobilität, hier insbesondere das Autofahren (AmI-Systeme erkennen Hindernisse, kontrollieren die Geschwindigkeit und verhindern das Abkommen von der Fahrbahn). In den Szenarien, die sich mit dem Autofahren befassen, wird in der Regel nicht thematisiert, welche Entscheidungsfreiheit die Anwender hinsichtlich ihres Transportmittels und der Reiseplanung haben. Bei den Gesundheitsszenarien stellt sich die Frage, ob die Überwachungs- und Diagnosesysteme ausreichend transparent für den typischen – meist älteren – Anwender sind, damit dieser nachvollziehen kann, welche Daten gesammelt, wo diese gespeichert, an wen sie übermittelt und wie sie verarbeitet werden.

Eine bedeutende Eigenschaft der AmI-Anwendungen mit einem hohen Kontrollgrad sind die weit reichenden Möglichkeiten zur Personalisierung, die zur Anpassung der jeweiligen Umweltbedingungen (Lichtverhältnisse, Raumtemperatur etc.) und zur Selektion von Informationsangeboten – Informationen über Produkte oder TV-Sendungen – genutzt werden können. In diesem Zusammenhang ist weniger die Frage des jeweiligen Kontrollniveaus entscheidend, sondern wer eigentlich die Kontrolle über das AmI-System ausübt. Mit Blick auf Produkt- und Serviceempfehlungen oder hinsichtlich personalisierter Informationsselektion stellt sich stets die Frage, wie die Interessen der Konsumenten geschützt werden und gewährleistet wird, dass die jeweiligen Auswahlkriterien einem bestimmten Mindestmaß an Objektivität gerecht werden. Verbraucherschützer melden jedenfalls ernsthafte Zweifel an hinsichtlich der Kontrollmöglichkeiten des Konsumenten bei AmI-Einkaufshilfen [AlM05]. Da Einzelhändler zugleich Eigentümer und Betreiber der AmI-Infrastruktur sind sowie Produkte und Dienstleistungen anbieten, ist die Vermutung naheliegend, dass sie den Konsumenten möglichst wenig Kontrolle über die AmI-Systeme überlassen wollen. Im Gegenzug besteht jedoch die Gefahr, dass Kunden aufgrund der asymmetrischen Verteilung der Kontrollrechte letztlich nicht oder nur sehr zögerlich bereit wären, entsprechende AmI-Angebote wahrzunehmen.

Auch mit Kommunikationsanwendungen in AmI-Systemen verbindet sich ein hoher Grad der Kontrolle. Zum einen verwalten AmI-Systeme die Kommunikationsverbindungen zwischen einer großen Zahl unterschiedlicher Netzwerke und passen die jeweiligen Informationen an die Anforderungen der unterschiedlichen Endgeräte an. Zum anderen wird in vielen Szenarien verdeutlicht, dass in bestimmten Ausnahmesituationen AmI-Systeme auf der Anwendungsebene ein ausgesprochen hohes Maß an Kontrolle ausüben. Dies betrifft beispielsweise Notfälle, in denen die Kommunikation zwischen der verletzten Person, der Rettungsleitstelle und den Notärzten, die auf dem Weg zum Unfallort sind, vollständig automatisiert abläuft. Manuelle Interventionen werden lediglich in einigen wenigen Fällen zugelassen und gehen selbst dann kaum über Empfangsbestätigungen hinaus. Notfallszenarien setzen somit eine ausgeklügelte Notfallkette und die vollständige Abdeckung eines Landes mit einer entsprechenden AmI-Infrastruktur voraus. Damit drängt sich indessen die Frage auf, ob diese Rettungssysteme auch dann funktionsfähig sind, wenn zentrale Systemkomponenten ausfallen (sei es durch Naturkatastrophen oder Anschläge). Falls nicht, leitet sich daraus die Forderung nach einer Absicherung durch robuste, möglichst redundante Kommunikationsprozeduren ab, die auf *low tech* basieren.

In einigen Szenarien werden auch Telefonverbindungen von AmI verwaltet. Dabei entscheidet das System, ob der Anruf an den Anwender durchgestellt wird oder nicht. Diese AmI-Funktionalität wird im ISTAG „Dimitrios"-Szenario besonders eindrucksvoll dargestellt: Der PDA ist sogar in der Lage, den Anwender zu imitieren und an dessen Stelle mit Anrufern zu kommunizieren. In jenen Szenarien, die „*Always-on*"-Video-Verbindungen zwischen unterschiedlichen Orten beschreiben, ist es in der Regel Sache des AmI-Systems, den Video-Link zu schließen, wenn beispielsweise die Kommunikation nach der Maßgabe vordefinierter Regeln unerwünscht oder unnötig ist oder gar eine potenzielle Verletzung der Privatsphäre darstellt.

In Szenarien über die Arbeitswelt werden AmI-Systeme im weitesten Sinne als Werkzeuge – etwa bei Simulationsverfahren oder zu Dokumentationszwecken – eingesetzt. Auch in diesen Fällen verbindet sich mit dem Einsatz von AmI-Systemen ein sehr hoher Grad der Kontrolle, da die Entscheidungen des Arbeitnehmers auf der Grundlage der Simulationsergebnisse sowie der automatischen Sitzungsmitschnitte getroffen werden. Obwohl AmI lediglich Simulationen produziert und die entsprechenden Schlussfolgerungen vom Individuum zu ziehen sind, werden grundsätzliche Fragen aufgeworfen, inwieweit und in welcher Qualität Simulationen die Komplexität real-weltlicher Zusammenhänge erfassen sowie unterschiedliche Situationen prognostizieren können und ob sich der Anwender nicht zu sehr auf maschinell erzeugte Simulationen verlässt und in der Folge Vorstellungskraft und Kreativität zu wenig nutzt.

### Informationsfluss

In der Mehrzahl der Szenarien erkennt die intelligente Umgebung den Benutzer, entweder zu Zwecken der Zugangskontrolle oder der Personalisierung. Es bleibt

jedoch überwiegend offen, wie die persönliche Identifikation exakt durchgeführt wird. Es gibt aber Hinweise, dass die Benutzer entweder über ein *identity token* verfügen, das automatisch vom System gelesen wird, oder biometrische Verfahren zum Einsatz kommen. Beide Möglichkeiten sind allerdings mit dem Risiko des Identitätsdiebstahls verbunden.

Szenarien, die Identifikation und Authentifizierung für hoch sicherheitsrelevante Anwendungen (Überwachung der Einwanderung, Schutz von Geschäftsgeheimnissen, Zugang zu Gesundheitsdaten) behandeln und dazu biometrische Sensoren vorsehen, beschreiben normalerweise nicht, welche Verfahren verwendet werden. Es ist allerdings wahrscheinlich, dass solche sicherheitskritischen Anwendungen mit Methoden wie dem Scannen von Iris oder Fingerabdrücken arbeiten werden. Damit ist der Diebstahl der Identität bzw. der biometrischen Daten auch mit einem hohen Risiko für Gesundheit und Leben verbunden.

Es ist zu beachten, dass Informationen, die zur Identifikation eines Nutzers verwendet werden, irgendwo (in einem persönlichen Gerät und/oder einer zentralen Datenbank) abgespeichert und im Zuge des Authentifizierungsvorgangs übermittelt werden müssen. Je größer die Zahl der Orte ist, an denen solche Informationen gespeichert werden, desto größer ist auch das Risiko, dass Unbefugte Zugriff darauf erhalten können. Dies gilt insbesondere, wenn Daten lokal auf einem PDA abgespeichert sind und dort entweder aus Gründen der technischen Leistungsfähigkeit des Gerätes oder purer Bequemlichkeit des Nutzers nicht hinreichend geschützt werden (können).

Ein weiteres sehr beliebtes Szenarienelement ist die Verfügbarkeit von Information über den Aufenthaltsort einer anderen Person oder eines Gegenstandes. Meist wird diese Information lokal, d.h. im Auto oder im persönlichen Endgerät verarbeitet, manchmal aber auch an einen Dienstanbieter übermittelt.

Das Nachverfolgen der Bewegungen von Arbeitskräften und arbeitsbezogenen Gegenständen wird in diesem Zusammenhang als eine übliche Funktionalität intelligenter Umgebungen dargestellt. Dabei wird die Ortsinformation häufig nicht lokal, sondern von einem zentralen Unternehmensserver verarbeitet oder gar gespeichert.

Ein weiteres recht gängiges Szenarioelement ist die automatisierte Bezahlung von Maut- und anderen Nutzergebühren, Waren und Dienstleistungen. Bei diesen Beispielen wird impliziert, dass Kreditkarteninformationen auf einem persönlichen Endgerät gespeichert sind und im Zuge einer finanziellen Transaktion automatisch übermittelt werden. Weitere vertrauliche Bankinformationen wie Kontostände u.Ä. sind den AmI-Systemen im Privathaushalt und am Arbeitsplatz ebenfalls bekannt.

Persönliche, hochsensible Informationen wie Krankheitsdaten werden entweder lokal auf einer *smart card* bzw. einem persönlichen Endgerät gespeichert – welches verloren gehen kann – oder liegen in einer zentralen Datenbank, die unter Umständen nicht ausreichend gesichert ist und arglistigen Arbeitgebern somit einen missbräuchlich Zugriff ermöglicht. Hinzu kommt, dass manche vertrauliche Informationen, wie beispielsweise Krankheitsdaten, von mehreren Stellen benötigt werden; entsprechend häufig sind Datentransfers gerade im Bereich der Gesundheitsdienste. Dies betrifft sowohl regelmäßige, automatisierte Datenübertragungen

neuer Sensordaten an die zentrale Datenbank, als auch umfangreiche Ad-hoc-Kommunikationen. Persönliche und tragbare AmI-Endgeräte kommunizieren mit den Systemen in der Arztpraxis oder im Krankenhaus, wobei ausgesprochen vertrauliche Informationen (persönliche Daten, Krankheitsgeschichte etc.) ausgetauscht werden. Mobile Notfallsysteme nutzen außerdem die Kommunikationssysteme Dritter als Relaisstationen, um Daten weiterzuleiten [SLK01]; im Rahmen eines Notrufs kann es somit vorkommen, dass persönliche Daten über die betroffenen Personen mehrere Übertragungspunkte und -systeme durchlaufen.

Weniger vertraulich, aber durchaus von hohem Interesse und wirtschaftlichem Wert für zahlreiche Organisationen und Firmen sind Daten, die zu Personalisierungszwecken gesammelt, entweder dezentral oder in einer Datenbank (etwa der Kundenkartei eines Einzelhändlers) gespeichert und häufig übermittel werden, um personalisierte Dienste anbieten zu können. Informationen solcher Art enthalten persönliche Nutzerprofile, die aus den gesammelten Daten über individuelles Einkaufs- und Freizeitverhalten, Informationspräferenzen aus der Internet- und TV-Nutzung sowie aus zahlreichen weiteren Kontexten erzeugt werden. Diese Daten offenbaren viel über die Vorlieben, den Lebensstil, den sozioökonomischen Status, den Gesundheitszustand etc. einer Person, insbesondere wenn sie mit den Daten aus anderen Quellen verknüpft werden. In diesem Zusammenhang ist zu betonen, dass Informationsflüsse zwischen Konsumenten und Anbietern in aller Regel asymmetrisch verlaufen: Kunden übermitteln ihre – sensiblen – persönlichen Daten an das AmI-Shoppingsystem, während das System umgekehrt lediglich unproblematische Produkt- und Preisinformationen zur Verfügung stellt.

Informationen über fachliche Qualifikation, meist in zentralen Datenbanken gespeichert, gelten in der Regel nicht als besonders schützenswert. Obwohl Informationen über Berufsqualifikation in der Tat weniger sensibel als identitätsbezogene Daten sind, sind sie für eine Vielzahl von Gruppen und Organisationen dennoch von herausragendem Interesse, da die Daten einerseits einen hohen wirtschaftlichen Wert darstellen und man andererseits keine kriminellen Motive verfolgen muss, um Vorteile aus ihrer Sammlung zu ziehen.

Die sicherlich am wenigsten sensiblen Informationen, die in den Szenarien gesammelt werden, sind Daten über die Infrastrukturen intelligenter Umgebungen, Ortsangaben von Objekten und Angaben über die Möglichkeiten zur Fernsteuerung der intelligenten Umgebungen. Allerdings können auch solche Informationen durchaus zur Planung und Durchführung krimineller oder gar terroristischer Aktivitäten nützlich sein. Da die PDAs nicht nur eine Fülle an Informationen über das Zuhause und die Haushaltsmitglieder speichern, sondern eben auch die Fernsteuerung des intelligenten Hauses ermöglichen, eröffnen sich vielfältige Gelegenheiten zur Manipulation und für arglistige Handlungen.

Zusammenfassend bleibt festzuhalten, dass unterschiedlichste personenbezogene Daten zunehmend unabhängig von Raum und Zeit erfasst werden können, da die Grenzen zwischen verschiedenen Kontexten immer mehr verwischt werden, wenn Menschen sowohl zu Hause arbeiten und von dort aus einkaufen oder von der Arbeit aus ihre Arzttermine vereinbaren sowie ihre Kinder beaufsichtigen und wenn die dauerhafte Überwachung und Speicherung individueller Handlungen zur Regel wird.

Die meisten Informationen über Identität, persönliche Eigenschaften, Gesundheit und Finanzen werden einerseits im Privathaushalt, also dort, wo sich Menschen in der Regel am sichersten fühlen, und andererseits in tragbaren AmI-Endgeräten gespeichert. Die Risiken, die mit einem Einbruch, einem Verlust oder einem Diebstahl verbunden sind, sind somit besonders hoch.

## Bedrohungen in einer Welt intelligenter Umgebungen

Die überwiegende Zahl der analysierten Szenarien geht davon aus, dass intelligente Umgebungen mit ihren Diensten breiten Bevölkerungsschichten einen erheblichen Mehrwert bringen und deswegen auch intensiv genutzt werden. Nur wenige Szenarien geben explizite Hinweise darauf, dass gleichzeitig auch bestimmte Risiken mit intelligenten Umgebungen verbunden sind, die gleichsam zwangsläufig als Preis für die Wohltaten einer Welt intelligenter Umgebungen zu zahlen sind. In praktisch all diesen Fällen wird thematisiert, dass für die Erbringung von intelligenten, personalisierten Diensten Daten über die Nutzer erhoben, gespeichert, verarbeitet und mit anderen Daten in Beziehung gebracht werden müssen. Einige dieser Gefahren werden allerdings bei der Analyse der Szenarien explizit oder implizit deutlich.

Generell tendieren die Menschen dazu, Technologien zu akzeptieren, ohne sich große Gedanken über Fragen des Datenschutzes zu machen, vorausgesetzt sie sind einfach zu bedienen und der Nutzen ist offenkundig (z. B. Nutzung von Mobiltelefonen trotz der Möglichkeit zur Feststellung des aktuellen Aufenthaltsorts oder die Nutzung von Kundenkarten trotz Offenlegung der persönlichen Konsumgewohnheiten) [Ham02].

Dennoch ist davon auszugehen, dass Datenschutzrisiken in einer Welt intelligenter Umgebungen zwangsläufig zunehmen werden und dass deswegen Datenschutzvorkehrungen bereits Bestandteil der technischen Systeme sein sollten, anstatt sich darauf zu verlassen, dass die späteren Nutzer schon sorgfältig mit ihren persönlichen Daten umgehen werden. Während man erfahrungsgemäß erwarten darf, dass sich eine gewisse öffentliche Aufmerksamkeit für Fragen der Datensammlung und der Kontrolle über diese Daten entwickeln wird, sollte man selbst den aufgeklärten Nutzern keine allzu große Last damit aufbürden, ständig entscheiden zu müssen, welche Daten sie von sich preisgeben, und die möglichen Konsequenzen dieser Entscheidung abzuschätzen [Win04].

Diese unübersichtliche Situation wird weiter dadurch verkompliziert, dass das Konzept der Privatsphäre und damit die Grundlage des Datenschutzes stark von der Kultur, der einzelnen Person sowie von der jeweiligen Situation abhängt. Die große Herausforderung für die künftige Welt intelligenter Umgebungen besteht somit darin, diese Vielfalt nicht zu beeinträchtigen, die das Herzstück unserer offenen Gesellschaften ausmacht [Roß05].

### Umfassende Überwachung

Die Verfügbarkeit von Daten über praktisch jeden Bürger kann auf staatlicher Seite Begehrlichkeiten in Bezug auf die Nutzung dieser Daten für Zwecke der Sozialversicherungen, der Strafverfolgung oder im Kampf gegen den internationalen Terrorismus wecken [Bül05]. Andere Institutionen wie Krankenversicherungen könnten ihre Datensammelaktivitäten ähnlich begründen. Da AmI-Anwendungen und -Dienste praktisch für alle Lebenssphären denkbar oder gar in Entwicklung sind – auch für solche, in denen der Schutz der Privatsphäre bislang unantastbar war wie etwa in Privatwohnungen –, kann es nicht überraschen, dass einige Kritiker intelligenter Umgebungen bereits das Gespenst eines Orwell'schen Überwachungsstaates umgehen sehen [AlM05].

Jenseits dieser Extremposition werden die zunehmenden Möglichkeiten zur Überwachung ganz konkrete Konsequenzen für die Bürger haben: Die Offenlegung von Gesundheitsdaten, persönlichen Vorlieben und Gewohnheiten gegenüber Versicherungsgesellschaften oder Arbeitgebern kann sehr leicht zu allen möglichen Formen der Diskriminierung führen (höhere Prämien, verminderte Karrierechancen oder gar Verlust von Versicherungsschutz oder Arbeitsplatz). Unabsehbar sind auch die möglichen Konsequenzen einer völligen Offenlegung solcher persönlicher Profile für familiäre und andere zwischenmenschliche Beziehungen. Schließlich eröffnen sie in kriminellen Händen die Möglichkeit für Straftaten wie Erpressung oder Betrug.

Besonders deutlich werden die möglichen Risiken, wenn man die höchst asymmetrischen Machtverhältnisse zwischen Anbietern und Kunden im Bereich des Einzelhandels betrachtet. Die dort erhobenen Daten können eben nicht nur zur Optimierung der Lieferketten genutzt werden, sondern machen den Einzelnen potenziell zum „gläsernen Konsumenten", der überwacht und gar manipuliert werden kann. So haben die Anbieter die Möglichkeit, bestimmten Kundengruppen besonders günstige Preisangebote zu machen, während andere Gruppen in dieser Hinsicht benachteiligt oder von bestimmten Angeboten gar vollständig ausgeschlossen werden. Da die technischen Systeme von den Anbietern aufgebaut und betrieben werden, bestehen für die Kunden normalerweise keine Verhandlungsmöglichkeiten. Es besteht also das Risiko, dass der versprochene wirtschaftliche Nutzen für die Kunden (Markt- und Preistransparenz) durch solche „Nebeneffekte" überkompensiert wird.

Einige der Szenarien führen an, es sei sinnvoll zu erfahren, wenn sich eine Bekannte oder ein Bekannter in der Nähe des eigenen Standorts aufhält. Selbst wenn dies richtig sein sollte, so stellt doch die Offenlegung persönlicher Lokationsdaten eine riskante Verletzung der Privatsphäre dar, da sie auch dazu genutzt werden können, die Wohnung von abwesenden Personen auszurauben oder ganz bestimmte Personen gezielt zu überfallen oder zu entführen. Im Extremfall könnte eine solche Funktion sogar dazu genutzt werden, sehr gezielte Terroranschläge durchzuführen.

Sogar einige auf den ersten Blick harmlose und ausschließlich nützliche Anwendungen können bei genauerem Hinsehen erhebliche Eingriffe in die Privatsphäre und die Menschenwürde darstellen. So berichtet Beckwith [Bec03], dass

Forscher ein „intelligentes Bett“ vorgeschlagen haben, das das Gewicht eines alten oder kranken Menschen überwacht. Während diese daran gedacht hatten, auf diese Weise einen unnatürlichen Gewichtsverlust feststellen und entsprechend medizinisch reagieren zu können, kann mit der gleichen Vorrichtung überwacht werden, wann die überwachte Person zu Bett geht und wieder aufsteht, ob sie einen ruhigen Schlaf hat und natürlich auch, wie viele Personen in dem Bett schlafen. Alle diese nicht vorgesehenen Nutzungen sind ethisch höchst problematisch.

### Identitätsdiebstahl

Unter Identitätsdiebstahl (*identity theft*) versteht man die missbräuchliche Nutzung personenbezogener Daten (der Identität) einer natürlichen Person durch Dritte. Ziel eines Identitätsdiebstahls ist es, einen finanziellen Vorteil zu erlangen, Daten der betroffenen Person an interessierte Kreise zu verkaufen oder den rechtmäßigen Inhaber der Identitätsdaten in Misskredit zu bringen [Elb05]. Je mehr personenbezogene Daten verfügbar sind, desto größer ist auch das Risiko des Identitätsdiebstahls. Dabei muss man unterscheiden, ob die Daten lokal auf einem Endgerät (einem Mobiltelefon, einem PDA) oder auf einem oder mehreren Servern bei einem Dienstleister gespeichert sind. Ein persönliches Endgerät kann gestohlen und wegen der nur schwachen (oft sogar ausgeschalteten) Schutzmechanismen leicht durch den Dieb verwendet werden – dafür ist der Schaden allerdings meist begrenzt. Server, auf denen personenbezogene Daten gespeichert sind, weisen meist sehr viel bessere Schutzmechanismen auf. Gelingt es einem Eindringling allerdings, diese zu überwinden, ist ein erheblicher Schaden möglich. Dieses Risiko wächst weiter, wenn Daten nicht nur bei einem, sondern bei mehreren Dienstleistern gespeichert werden. Sobald sich der Identitätsdieb im Besitz bestimmter persönlicher Daten befindet, können diese dazu verwendet werden, weitere sensible Daten einer Person auszuspionieren und diese dann für jede Art von Betrug und sogar für die Durchführung terroristischer Akte zu nutzen.

Erschwerend kommt hinzu, dass eine Information nicht einmal physisch gestohlen werden muss, weil auch eine Kopie der Information ausreichend ist. Darüber hinaus muss die gestohlene Information auch nicht in einer physischen Weise genutzt werden. Tatsächlich kann ein Identitätsbetrug auch vollkommen anonym verübt werden (etwa über das Internet oder per Telefon). Im Unterschied zu früher muss kein Kunde mehr einen Laden betreten, um einen Betrug zu begehen. Die technischen Möglichkeiten machen Betrug heute so einfach wie nie zuvor, und die Risiken, bei einem Identitätsdiebstahl gefasst zu werden, sind denkbar gering.

Die Verfahren zum Identitätsdiebstahl sind vielfältig und können sowohl online als auch offline sein. Zu den klassischen Offline-Verfahren gehört der Diebstahl von Geldbörsen und Brieftaschen, die Suche nach privaten Zugangsdaten durch Stöbern in Wohnungen und Autos, das heimliche Öffnen oder Stehlen von Briefen, betrügerische Anrufe usw. Die Online-Methoden umfassen Angriffe auf Computer, Online-Accounts oder PDAs (s.u.), das Abfangen von Finanztransaktionen, betrügerische Websites und E-Mails mit fingierten Kennwortabfragen, Phishing usw. Die Liste der Verfahren für den Identitätsdiebstahl ist lang, und bei je-

der technischen Neuentwicklung werden neue Sicherheitslücken zu diesem Zweck genutzt. Meist bleibt (zumindest bei den Online-Verfahren) der Identitätsdiebstahl zunächst unentdeckt, manchmal bleiben die betroffenen Personen sogar noch arglos, wenn bereits erste Fälle betrügerischen Auftretens stattgefunden haben.

### Bösartige Angriffe

Unter dem Begriff „bösartiger Angriff" (*malicious attack*) wird eine Reihe von Verfahren zusammengefasst, durch die Personen versuchen, Zugriff zu einem Computer, Mobiltelefon oder sonstigen Endgeräten zu erhalten, entweder um Daten zu entwenden oder um das Gerät zu beschädigen bzw. außer Betrieb zu setzen. Hierfür gibt es vielfältige Möglichkeiten sowohl aktiver als auch passiver Art. Bei einem aktiven Angriff werden absichtlich bestimmte Daten verändert bzw. gelöscht oder falsche Daten neu erzeugt. Bei einem passiven Angriff werden Daten zwar heimlich mitgelesen oder kopiert, nicht aber geändert oder gelöscht.

Gerade komplexe technische Systeme, so wie sie in den meisten Szenarien beschrieben werden, können zu einem bevorzugten Objekt für aktive Viren- oder *Denial-of-Service*-Angriffe werden, die eine Fehlfunktion oder einen teilweisen oder kompletten Ausfall des technischen Systems nach sich ziehen können. Die Folgen eines solchen Versagens reichen von einem Verlust an Bequemlichkeit bis zu gravierenden (finanziellen und körperlichen) Schäden. Im Falle kritischer Infrastrukturen kann es sogar zu nachhaltigen Versorgungsengpässen oder erheblichen Störungen der öffentlichen Sicherheit kommen. Dabei stellt sich auch die Frage, wer für die unmittelbaren, vor allem aber die mittelbaren Folgen eines solchen Systemversagens haftbar ist.

Mit der Verbreitung intelligenter Umgebungen und der „Veralltäglichung" ihrer Nutzung in vielen Lebensbereichen wird die Abhängigkeit des Einzelnen aber auch der Wirtschaft und Gesellschaft als Ganzes erheblich davon abhängen, dass das technische System hochgradig zuverlässig und verfügbar ist. Da ein erfolgreicher Angriff auf diese (Infrastruktur-)Systeme zu einem zeitweisen Zusammenbruch der wirtschaftlichen und gesellschaftlichen Aktivitäten führen kann, sind zuverlässige und effiziente Verfahren zur Systemdiagnose aber auch die Existenz eines technischen und/oder nicht-technischen Sicherungssystems notwendig.

### Digitale Spaltung der Gesellschaft

Die Durchdringung praktisch aller Lebensbereiche mit AmI-Anwendungen birgt die Gefahr des sozialen Drucks und der digitalen Spaltung der Gesellschaft. So könnten viele Menschen gezwungen sein, die neue Technologie anzuwenden, um wichtige Dienste überhaupt nutzen und am gesellschaftlichen Leben teilnehmen zu können. Beispielsweise könnte die Gewährung einer Krankenversicherung unmittelbar davon abhängig gemacht werden, dass die Person irgendeine Art von technischer Überwachung ihrer Vitalfunktionen nutzt. Oder aber es wird ein indirekter Druck zur Verwendung der Technik ausgeübt, weil es neben der techni-

schen Lösung keine andere Möglichkeit (mehr) gibt, bestimmte Dienstleistungen überhaupt zu nutzen, so dass letztlich gar keine echte Wahlmöglichkeit mehr besteht [Sch05]. Aber auch wenn eine Person sich auf die Nutzung der Technologie einlässt, kommt es eventuell zu einer Einschränkung der persönlichen Entscheidungsfreiheit, da die vom System vorgesehenen Handlungsdispositionen bereits durch andere Menschen vorstrukturiert, interpretiert und bewertet wurden [Hee05]. Die Nichtverfügbarkeit des Systems für Nicht-Routineaufgaben sowie die Möglichkeit der Fehlinterpretation menschlicher Eingaben können darüber hinaus auch die individuelle Entwicklung des Benutzers in persönlicher, sozialer oder beruflicher Hinsicht negativ beeinflussen.

Die Abhängigkeit von technisch vermittelter Kommunikation und automatisierter medizinischer Versorgung führt darüber hinaus zur Abnahme persönlicher Kontakte mit dem Risiko, dass insbesondere ältere Personen vereinsamen, keine neuen sozialen Kontakte aufbauen können oder gar das Vertrauen in die zu ihrem Nutzen entwickelte Technik verlieren.

Schließlich besteht die Gefahr, dass Kinder und Jugendliche nur unzureichend auf die Herausforderungen des Lebens vorbereitet sind, wenn sie zu viel Zeit in virtuellen Welten verbringen oder unter ständiger Überwachung der Eltern stehen. Dies kann sich beispielsweise durch mangelnde Kommunikationsfähigkeit und Eigenverantwortlichkeit oder der Unfähigkeit zum Alleinsein äußern.

Weil viele Funktionen des täglichen Lebens von AmI-Diensten abhängig würden, könnten die Menschen auch darin behindert werden, sich persönlich fortzuentwickeln oder selbstständig im täglichen Leben zurechtzukommen. Dies kann letztlich zu einem Verlust von Selbstvertrauen und zu Depressionen führen.

Die Verbreitung intelligenter Umgebungen stellt auch die Beziehungen zwischen Mitgliedern sozialer Gruppen, insbesondere in der Familie, in Frage. So gibt die AmI-Technologie den Eltern ein mächtiges Werkzeug zur Überwachung und Kontrolle ihrer Kinder an die Hand. Dies wirft unmittelbar die Frage auf, ab welchem Alter die Privatsphäre der Kinder gegenüber den Eltern geschützt sein sollte, um die persönliche Entwicklung nicht zu behindern und wer die Grenzen dieser Privatsphäre definieren sollte. Die Familie selbst oder der Staat?

Zuletzt werden auch AmI-Anwendungen und -Dienste nicht kostenfrei angeboten werden können, so dass nicht alle Bürger in gleicher Weise von den Möglichkeiten der Technologie profitieren werden – auch oder gerade in Bereichen, die bislang als öffentliches Gut gelten. Dies gilt insbesondere für das Gebiet der Bildung, wo es durch eine Ökonomisierung der Angebote zu einer stärkeren Trennung zwischen gut ausgebildeten und weniger gut ausgebildeten Bevölkerungsschichten kommen kann.

## Schlussfolgerungen

Die wesentliche Schlussfolgerung unserer Analyse besagt, dass AmI-Technologie das Potenzial besitzt, die meisten der heute existierenden Grenzen der Privatsphäre und des Datenschutzes zu überschreiten.

Erstens werden die physischen Grenzen der Beobachtbarkeit und der Privatsphäre durch die zunehmende Konnektivität von Menschen und Räumen immer stärker verwischt. Ein bekanntes Beispiel für dieses Phänomen sind Experimente im Umfeld des computerunterstützten kooperativen Arbeitens (*Computer-Supported Cooperative Work*, CSCW), bei denen in den Büros der Testpersonen Kameras installiert werden, um die Aufmerksamkeit zwischen den Mitarbeitern zu erhöhen und eine natürlichere und häufigere Kommunikation zwischen ihnen zu ermöglichen. Diese Experimente haben gezeigt, dass Menschen mit der Zeit nicht mehr wahrnehmen, dass sie ständig per Videokamera überwacht werden, weil die intuitive Erwartung „wenn ich dich nicht sehen kann, kannst du mich auch nicht sehen" in der Realität des computergestützten kooperativen Arbeitens nicht zutrifft [BeS93] und dies die Privatsphäre gefährdet, die auch im Arbeitsumfeld (eingeschränkt) geschützt ist.

Zweitens machen physiologische Sensoren, die ständig vom Menschen getragen werden und kontinuierlich Messdaten produzieren (sei es, um den Gesundheitszustand zu überwachen oder um Fernseh- oder Lernprogramme zu personalisieren), es der betroffenen Person unmöglich, ihre Gefühle zu verbergen, weil diese sich aus den Veränderungen der physiologischen Parameter ableiten lassen [NAL03]. Dies bedeutet, dass der Gesichtsausdruck und die Körpersprache nicht mehr länger eine natürliche Grenze für die inneren Regungen des Menschen darstellen.

Drittens führen das Verwischen der Grenzen von Raum und Zeit, die Möglichkeit zum Aufnehmen und Speichern von einer Vielzahl von Datentypen sowie die zunehmende Leistungsfähigkeit von Verfahren des *Data Mining* (mit denen es möglich wird, in einem großen Datenbestand implizite Verbindungen zwischen a priori unverbundenen Daten zu ermitteln) zu einer Verletzung der persönlichen Erwartungen an die Schutzwirkung von räumlichen und zeitlichen Grenzen der Privatsphäre. Auch die Grenzen der Privatsphäre aufgrund klassischerweise kurzlebiger oder vorübergehender Effekte werden auf diese Weise unterminiert.

Schließlich verändern neue Technologien immer wieder ganz grundsätzlich die Vorstellung über die Privatsphäre und deren Schutz. Nissenbaum [Nis04] führt beispielsweise eine US-Gerichtsentscheidung für einen solchen Fall an. Das Gericht hatte entschieden, dass die Polizei nicht die Privatsphäre einer Person verletzt, wenn sie beim Überflug über das Haus und Privatgrundstück dieser Person eine Straftat entdeckt. Man dürfe beim Überflug eines Überwachungsflugzeugs keinerlei Schutz der Privatsphäre erwarten, da Flugzeugüberflüge über Privatgelände zum festen Bestandteil des täglichen Lebens geworden seien.

Es bleibt somit die Frage, welche geänderten Erwartungen im Hinblick auf den Schutz der Privatsphäre bzw. persönlicher Daten sich durchsetzen werden, wenn intelligente Umgebungen zu einem selbstverständlichen Teil unseres täglichen Lebens werden. Wie immer diese Erwartungen aussehen mögen – sie werden sich jedenfalls viel langsamer entwickeln als das Leistungsvermögen der zu Grunde liegenden Technologie.

**Dank.** Dieser Beitrag entstand im Rahmen des von der Europäischen Kommission geförderten Projekts SWAMI: Safeguards in a World of Ambient Intelligence (http://swami.jrc.es). Er gibt die Meinung der Autoren wieder, die nicht notwendigerweise der Meinung der Europäischen Kommission entspricht. Die Autoren danken den Projektpartnern für ihre Beiträge zu diesem Text.

## Literatur

[AaM03] Aarts E, Marzano S (Eds.) (2003) The New Everyday: Views on Ambient Intelligence. Uitgeverij 010 Publishers, Rotterdam

[Ack04] Ackerman MS (2004) Privacy in pervasive environments: next generation labelling protocols. Personal and Ubiquitous Computing 8(6) 430-439

[AHC01] Åkesson K-P, Humble J, Crabtree A, Bullock A (2001) Usage and Development Scenarios for the Tangible Toolbox. ACCORD Deliverable D1.3. Swedish Institute of Computer Science, Kista, www.sics.se/accord/plan/del/D1.3.pdf

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

[AsH02] Aschmoneit P, Höbig M (2002) Context-Aware Collaborative Environments for Next Generation Business Networks: Scenario Document. COCONET deliverable D 2.2. Enschede: Telematica Institute

[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

[Bec03] Beckwith R (2003) Designing for Ubiquity: The Perception of Privacy. IEEE Pervasive Computing 2(2) 40-46

[BeS93] Bellotti V, Sellen A (1993) Design for Privacy in Ubiquitous Computing Environments. Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93) 77-92

[Bül05] Bülligen F (2005) Vorratsdatenspeicherung von Telekommunikationsdaten im internationalen Vergleich: Stand und Perspektiven – Zur Konstitution einer neuen politischen Arena. DuD – Datenschutz und Datensicherheit 29(6) 349-353

[CaR05] Cabrera Giráldez M, Rodríguez Casal C (2005) The Role of Ambient Intelligence in the Social Integration of the Elderly. In: Riva G, Vatalaro F, Davide F, Alcañiz M (Eds.): Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction, IOS Press, 265-280

[Cas04] Casert R (2004). Workshop Ambient Intelligence: In the service of Man? Societal aspects of ambient intelligence in the field of health and surveillance. Rathenau Institute

[Elb05] Elbirt AJ (2005) Who Are You? How to Protect Against Identity Theft. IEEE Technology and Society Magazine 24(2) 5-8

[FDP05] Friedewald M, Da Costa O, Punie Y, Alahuhta P, Heinonen S (2005) Perspectives of Ambient Intelligence in the Home Environment. Telematics and Informatics 22(3) 221-238

[Ham02] Hameling CJ (2002) Risks in the Global e-Society. In: Banse G, Grunwald A, Rader M (Eds.): Innovations for an e-Society – Challenges for Technology Assessment, Edition Sigma, 57-66

[Har05] Harrop P (2005) Item level RFID: The business benefits of the "tag everything" scenario. IDTechEx Ltd, Cambridge

[Hee05] Heesen J (2005) Ubiquitous Computing als subjektorientierte Technikvision. In: Bora A, Decker M, Grunwald A, Renn O (Eds.): Technik in einer fragilen Welt: Die Rolle der Technikfolgenabschätzung, Edition Sigma, Berlin, 183-191

[Hei04] Heinonen S (2004) Mobile Telework at the Crossroads of Social, Environmental and Cultural Challenges. In: 9th International Telework Workshop, International Telework Academy, Crete, Greece, 6th - 9th September, 2004

[IDB01] IST Advisory Group, Ducatel K, Bogdanowicz M, Scapolo F, Leijten J, Burgelman JC (2001) Scenarios for Ambient Intelligence in 2010, Institute for Prospective Technological Studies (IPTS), Sevilla

[ITE04] ITEA Technology Roadmap for Software-Intensive Systems, 2nd edition (2004) Information Technology for European Advancement (ITEA) Office Association, Eindhoven

[JDS04] Jafari R, Dabiri F, Sarrafzadeh M (2004) Reconfigurable Fabric Vest for Fatal Heart Disease Prevention. In: UbiHealth 2004 – The 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Nottingham, 7 September 2004

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

[LHN04] Luff P, Heath C, Norrie M, Signer B, Herdman P (2004) Only touching the surface: Creating affinities between digital content and paper. In: Proceedings of the 2004 ACM conference on computer supported cooperative work, Chicago, USA, 8th – 10th November 2004, 523-532

[LMP03] Luck M, McBurney P, Preist C (2003) Agent Technology: Enabling Next Generation Computing. A Roadmap for Agent Based Computing, AgentLink, Southampton

[Lop04] López de Vallejo IL (2004) E-Locus: A clustered view of European ICT for future workspaces. E-Locus Deliverable D5.5. Fundación TEKNIKER, Guipúzcoa

[MaB03] Masera M, Bloomfeld R (2003) A Dependability Roadmap for the Information Society in Europe. AMSD Deliverable D1.1. Rand Europe, Leiden, https://rami.jrc.it/roadmaps/amsd

[MMS03] Michahelles F, Matter P, Schmidt A, Schiele B (2003) Applying Wearable Sensors to Avalanche Rescue: First Experiences with a Novel Avalanche Beacon. Computers & Graphics 27(6) 839-847

[MoR05] Morganti F, Riva G (2005) Ambient Intelligence for Rehabilitation. In: Riva G, Vatalaro F, Davide F, Alcañiz M (Eds.) Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction. IOS Press, Amsterdam, 281-292

[MYA05] Ma J, Yang LT, Apduhan BO, Huang R, Barolli L, Takizawa M (2005) Towards a Smart World and Ubiquitous Intelligence: A Walkthrough from Smart Things to Smart Hyperspaces and UbiKids. International Journal of Pervasive Computing and Communications 1(1)

[NAL03] Nasoz F, Alvarez K, Lisetti C, Finkelstein N (2003) Emotion Recognition from Physiological Signals for User Modelling of Affect. In: Proceedings of the 3rd Workshop on Affective and Attitude User Modelling, Pittsburgh, USA, June 2003

[Nis04] Nissenbaum H (2004) Privacy as Contextual Integrity. Washington Law Review 79(1) 101-139

[ORB99] Orr RJ, Raymond R, Berman J, Seay F (1999) A System for Finding Frequently Lost Objects in the Home. Technical Report 99-24. Graphics, Visualization, and Usability Center, Georgia Tech, Atlanta

[PTA01] Palmas G, Tsapatsoulis N, Apolloni B, Malchiodi D, Delopoulos A, Beverina F (2001) Generic Artefacts Specification and Acceptance Criteria. Oresteia Deliverable D01. STMicroelectronics s.r.l, Milano

[RFE05] Remagnino P, Foresti GL, Ellis T (Eds.) (2005) Ambient Intelligence: A Novel Paradigm. Springer, Boston

[Riv03] Riva G (2003) Ambient Intelligence in Health Care. CyberPsychology and Behavior 6(3) 295-300

[Roß05] Roßnagel A (2005) Verantwortung für Datenschutz. Informatik-Spktrum 28(6) 462-473

[Sch05] Scheule RM (2005) Das „Digitale Gefälle" als Gerechtigkeitsproblem. Informatik-Spektrum 28(6) 474-488

[Sin01] Singer I (2001) Privacy and Human Nature. Ends and Means 5(1)

[SLK01] Savidis A, Lalis S, Karypidis A, Georgalis Y, Pachoulakis Y, Gutknecht J, Egger B, Kramer P, Tafra M, Majoe D, Lieu V, Hunt N, Gredmaier L, Roberts D (2001) Report on Key Reference Scenarios. 2WEAR Deliverable D1. Foundation for Research and Technology Hellas, Institute of Computer Science, Heraklion

[VLN04] Van Laerhoven K, Lo BPL, Ng JWP, Thiemjarus S, King R, Kwan S, Gellersen H, Sloman M, Wells M, Needham P, Peters N, Darzi A, Toumazou C, Yang GZ (2004) Medical Healthcare Monitoring with Wearable and Implantable Sensors. In: UbiHealth 2004 – The 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Nottingham, 7 September 2004

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

[Win04] Winters N (2004) Personal Privacy and Popular Ubiquitous Technology. In: Proceedings of Ubiconf 2004, Gresham College, London, 19 April 2004

**Dr. Michael Friedewald** hat an der Rheinisch-Westfälischen Technischen Hochschule Aachen Elektrotechnik, Wirtschaftswissenschaften und Technikgeschichte studiert. Seit 1999 ist er als Projektleiter am Fraunhofer-Institut für System- und Innovationsforschung in Karlsruhe tätig. Seine Arbeitsschwerpunkte liegen im Bereich der Mediennutzungsforschung und der Technikfolgenabschätzung, insbesondere im Bereich Ambient Intelligence.

**Dr. Ralf Lindner** studierte Politikwissenschaft und Volkswirtschaftslehre an der Universität Augsburg und der University of British Columbia, Vancouver. In seiner Dissertation befasste er sich mit der strategischen Anwendung neuer Informations- und Kommunikationstechnologien durch intermediäre Organisationen. Seit 2005 ist er als Projektleiter am Fraunhofer Institut für System- und Innovationsforschung, Abteilung „Neue Technologien", tätig. Neben der Analyse von Diffusionsprozessen neuer Technologien liegen seine Forschungsinteressen im Bereich von Politikfeldanalysen (insbesondere Medien-, Forschungs- und Technologiepolitik).