Gesellschaftliche Herausforderungen durch „intelligente Umgebungen“

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

Mit der umfassenden drahtlosen Vernetzung und Computerisierung von Alltagsgegenständen und Umgebungen werden nicht nur neuartige Anwendungen möglich, sondern auch zahlreiche Risiken erzeugt. Soll Ambient Intelligence (AmI) ein Erfolg werden, ist es erforderlich, angemessene Maßnahmen zu ergreifen, um Privatsphäre, Sicherheit oder Vertrauen in den jeweiligen Anwendungskontexten zu gewährleisten. Dabei besteht die Herausforderung darin, frühzeitig Vorkehrungen gegen Risiken zu entwickeln, die noch nicht manifest sind. Im Rahmen des EU-Projekts „Safeguards in a World of Ambient Intelligence“ wurden Szenarien entwickelt, mit deren Hilfe potenzielle Risiken in einer frühen Phase der Technikentwicklung identifiziert wurden.[1] Der Beitrag skizziert die angewandte Szenarienmethode, präsentiert die zentralen Befunde und stellt darüber hinaus kurz mögliche Gegenmaßnahmen vor.

1 Einleitung

Die Vision der Ambient Intelligence („intelligente Umgebungen“) postuliert eine künftige Gesellschaft, in der die Menschen von quasi autonomen und im Hintergrund agierenden Assistenzsystemen umgeben sind, die sich proaktiv auf die Bedürfnisse des Nutzers einstellen und dabei weitgehend ohne herkömmliche Mensch-Maschine-Schnittstellen auskommen. Angestrebt wird eine draht- und nahtlose Vernetzung von Alltagsgegenständen und Umgebungen, die mit rechnergestützten Sensoren und Aktuatoren versehen sind. Der Begriff Ambient Intelligence (AmI), der ursprünglich auf Emile Aarts von Philips Research zurück geht (vgl. Aarts, Appelo 1999), wurde bald von der Information Society Technologies Advisory Group der EU aufgegriffen (ISTAG 2001) und als ein Schwerpunkt des Fünften Forschungsrahmenprogramms integriert. Wesentliche Elemente der Zukunftsvision AmI basieren auf Mark Weisers paradigmatischem Konzept des Ubiquitous Computing, das dieser Ende der 1980er Jahre am Xerox Palo Alto Research Center (Parc) entwarf. In einem viel beachteten Zeitschriftenbeitrag beschreibt Weiser (1991) Ubiquitous Computing als dritte Generation von Computersystemen – nach Großrechnern und PCs –, die sich insbesondere dadurch auszeichne, dass Datenverarbeitung zu einem integralen und weitgehend unsichtbaren, aber für den Menschen leicht zugänglichen Bestandteil des Alltags wird (Weiser 1991, S. 92). Der Grundgedanke der unmerklichen Durchdringung der dinglichen Welt mit Informations- und Kommunikationstechnologien („Heinzelmännchen-Technologie“) ist seither in zahlreichen Varianten fortentwickelt worden.

Der normative Gehalt der explizit nutzerzentrierten AmI-Vision (vgl. Punie 2005, S. 113) besteht in der Erwartung positiver Auswirkungen der Technologie auf die individuelle Lebensqualität – und zwar in nahezu sämtlichen lebensweltlichen Kontexten. In dem Maße jedoch, wie die allgegenwärtigen personalisierten Dienste und Anwendungen von AmI in das alltägliche Leben integriert werden, erhöht sich nicht nur der persönliche Komfort, die Kommunikations- und Leistungsfähigkeit, sondern es ergeben sich mit Blick auf Privatsphäre, Identität, Datenschutz und -sicherheit zahlreiche problematische Implikationen und potenzielle Gefahren. Die möglichen Risiken beruhen insbesondere darauf, dass

- ein Großteil der individuellen Alltagsaktivitäten erfasst, gespeichert, verarbeitet und innerhalb der allgegenwärtigen Netzwerke übermittelt wird, um die vorgesehenen personalisierten Dienste zu ermöglichen;
- sich somit die *Quantität* der in Umlauf befindlichen personenbezogenen Daten dramatisch steigern wird und die Daten zudem in wachsendem Maße miteinander verknüpft und ggf. zweit- und mehrfach verwertet werden können;
- sich die *Qualität* der personenbezogenen Daten aufgrund des Einsatzes von Kameras, Wahrnehmungssensoren und biometrischen Verfahren tief greifend wandeln wird.

Mit diesen und ähnlichen Fragen befasste sich das im August 2006 abgeschlossene For-

schungsprojekt Safeguards in a World of Ambient Intelligence (SWAMI), dessen Aufgabe es war, politische Handlungsoptionen und Forschungserfordernisse zu identifizieren, um den gesellschaftlichen, rechtlichen und organisatorischen Implikationen von AmI angemessen zu begegnen. Wichtigstes methodische Instrument des Projekts war die Entwicklung von sogenannten „dunklen Szenarien", anhand derer zentrale Schwachstellen und Risikobereiche künftiger AmI-Anwendungen möglichst realistisch herausgearbeitet werden sollten.

Dieser Beitrag unterstreicht die Notwendigkeit, dass Szenarien über zukünftige Technikentwicklungen eine größere Realitätsnähe anstreben sollten, indem nicht nur die erwünschten Auswirkungen einer technologischen Innovation, sondern eben auch die denkbaren Schattenseiten systematisch herausgearbeitet werden. Im Folgenden wird ein solch realistischer Szenarien-Ansatz vorgestellt.

2 Dunkle Szenarien

Die Entwicklung von Szenarien gehört zu den wichtigsten Foresight-Methoden. Die AmI-Vision selbst wurde frühzeitig von unterschiedlichen Akteuren aufgegriffen und in einer Vielzahl von Zukunftsszenarien ausgemalt und weiterentwickelt (z. B. ISTAG 2001). Bekanntlich stellen Szenarien keine Vorhersagen dar, vielmehr werfen sie Schlaglichter auf mögliche künftige Entwicklungen und zeigen Wege auf, wie diese realisiert werden können. Ihre Funktion liegt dabei vor allem in der Stimulierung von Debatten, der Strukturierung von Denkfiguren und der Unterstützung bei der Synthetisierung möglichst realistischer Zukunftspläne (vgl. Ringland 1998; Godet 2000; Gavigan et al. 2001).

Viele Szenarien-Prozesse und Foresight-Studien zielen darauf ab, möglichst erstrebenswerte Zukunftsbilder zu entwerfen – eine Beobachtung, die gleichfalls für die Mehrzahl der Szenarien im Bereich von AmI gilt (vgl. Friedewald, Lindner 2007). Dieser positive Ansatz ist legitim und erfüllt zudem wichtige Funktionen bei der zielgerichteten Ausgestaltung von Forschungs- und Entwicklungsprozessen. Sogenannte „dunkle Szenarien" repräsentieren hingegen Zukunftsbilder, die sich aus einer normativen Perspektive grundsätzlich *nicht* realisieren sollten. Indem sie sich auf die wahrscheinlichen, aber häufig nicht bedachten negativen Auswirkungen der Anwendung von AmI-Technologien konzentrieren, beschreiben sie eine Zukunft, die durchaus Realität werden könnte, sollten keine geeigneten Vorkehrungen ergriffen werden. Sie stellen damit ein nützliches Instrument einer prospektiven Technikfolgenabschätzung dar.

Am Beginn der eigentlichen Szenarien-Entwicklung von SWAMI stand die Identifizierung potenzieller Schwachstellen und Risiken von AmI. Dabei ist zu betonen, dass die dunklen Szenarien, die im Rahmen des Projekts konzipiert wurden, keineswegs sämtliche hypothetischen Fehlentwicklungen aufgreifen, die unter AmI aus heutiger Warte auftreten könnten. Auch sind die dunklen Szenarien nicht mit der Intention entworfen worden, Positionen zu stärken, die technologischen Fortschritt im Allgemeinen und AmI im Besonderen pauschal ablehnen. Im Gegenteil, explizites Ziel des Szenarien-Prozesses war es, frühzeitig auf mögliche Fehlentwicklungen aufmerksam zu machen und entsprechende Maßnahmen zu entwickeln und anzuregen, damit die dunklen Zukunftsbilder erst gar nicht eintreten. Ein weiterer zentraler Arbeitsschritt des SWAMI-Projekts bestand daher in der Identifizierung geeigneter Schutzmaßnahmen, um den zahlreichen Risiken von AmI wirksam begegnen zu können.

Diese Identifizierung von Gefährdungen und der entsprechenden Schutzvorkehrungen ähnelt Ansätzen, wie sie in der klassischen Risikoanalyse und -bewertung angewandt werden (vgl. Renn, Zwick 1997; Klinke, Renn 2001). Hier wie dort werden Gefahren und schützenswerte Güter identifiziert, Ausmaß und Wahrscheinlichkeit unerwünschter Folgen bestimmt und entschieden, welche Vorsichtsmaßnahmen zu ergreifen sind.

Bei den SWAMI-Szenarien handelt es sich um sogenannte Trendszenarien (vgl. Massini, Vasquez 2000). Sie basieren auf Extrapolationen aktueller Entwicklungen; der eigentliche Szenarien-Prozess beginnt in der Gegenwart und tastet sich in eine möglichst realitätsnahe Zukunft vor. Extreme und damit ausgesprochen unwahrscheinliche Zukunftsentwürfe sollen damit nicht entwickelt werden.

3 Vier Szenarien einer Welt mit intelligenten Umgebungen

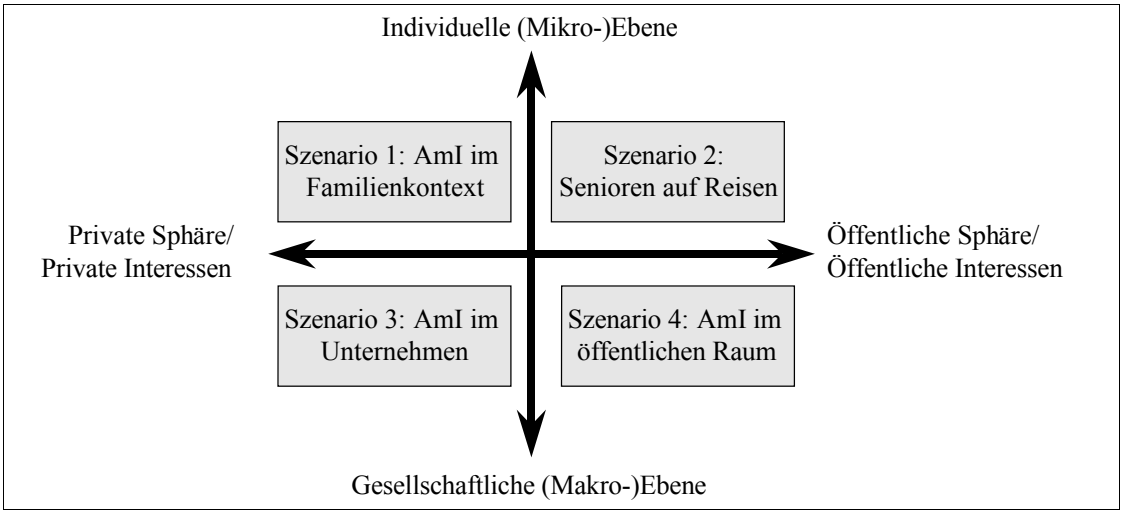
Insgesamt wurden vier dunkle Szenarien entwickelt, um einen handhabbaren Kompromiss angesichts erwünschter Vielfalt und limitierter Ressourcen einzugehen. Der eigentliche Szenarien-Prozess bestand in einer Kombination aus Literaturanalysen und interaktiven Workshops, an denen sowohl das SWAMI-Konsortium als auch geladene Experten beteiligt waren.[2]

Um mit lediglich vier Szenarien ein möglichst umfassendes und vielschichtiges Problemspektrum abdecken zu können, orientierte sich die Ausgestaltung von Situationen sowie die Bestimmung von Kontexten und handelnden Personen an einem zweidimensionalen Analysefeld (vgl. van 't Klooster, van Asselt 2006). Die vertikale Achse differenziert zwischen Situationen, die eher auf der Makro- oder der Mikroebene angesiedelt sind, während die horizontale Achse zwischen Problemen unterscheidet, die eher einen Bezug zu privaten Belangen bzw. eine gesamtgesellschaftliche Relevanz aufweisen (siehe Abb. 1).

Obwohl die Szenarien sowohl individuelle und gesellschaftliche als auch private wie öffentliche Belange thematisieren, wurde versucht, die Szenarien-Geschichten jeweils aus der Perspektive des Alltags eines individuellen Nutzers bzw. Betroffenen zu erzählen:[3]

1. *Eine typische Familie mit Situationen in verschiedenen Kontexten*: Hier werden Schwachstellen von AmI veranschaulicht, die sich auf das Leben einer „normalen" Familie auswirken können. Die unerwünschten Situationen treten in unterschiedlichen Kontexten auf (im intelligenten Haus, am Arbeitsplatz, im öffentlichen Park).
2. *Senioren auf Reisen*: Durch eine illegale Manipulation an einem elektronischen Verkehrsleitsystem werden ältere Mitbürger in einen Unfall verwickelt, bei dem auch Mitglieder der Reisegruppe zu Schaden kommen. Verschiedene Situationen mit Blick auf Reisen, Kommunikation und Gesundheitsversorgung werden im Szenario behandelt.
3. *Vorstandssitzung eines internationalen Konzerns und gerichtliches Nachspiel*: Ein Unternehmen, dessen Geschäftsmodell auf der Sammlung, der Aggregation und dem Verkauf personenbezogener Daten basiert, wird Opfer eines groß angelegten Datendiebstahls. Die Vertuschungsversuche der Unternehmensleitung werden in einem späteren Gerichtsverfahren aufgearbeitet.
4. *Facetten der Risikogesellschaft*: Aus der Perspektive einer Nachrichtensendung werden vier gesellschaftliche Problemfelder beleuchtet, in denen AmI eine Rolle spielt. Aufhänger sind die Forderungen einer Interessengruppe, die sich gegen personalisiertes Profiling wendet, die digitale Spaltung und Umweltprobleme im globalen Maßstab; die Schwachstellen von technischen Verkehrsüberwachungssystemen und schließ-

Abb. 1: Positionierung der Szenarien



Quelle: Eigene Darstellung

lich nichtintendierte Wirkungen von AmI-Systemen zur Sicherung von Massenveranstaltungen.

4 Herausforderungen durch intelligente Umgebungen

Die Analyse der einzelnen Szenarien-Situationen förderte eine große Bandbreite an Themen und Problembereichen zutage. Zur besseren Veranschaulichung werden im Folgenden vier dieser Schlüsselthemen anhand von Beispielsituationen aus den Szenarien kurz dargestellt:

Identität

Viele Internetnutzer verwenden dasselbe Passwort und / oder dieselbe Benutzerkennung für unterschiedliche Internetseiten und Systeme. Ob beabsichtigt oder nicht, die meisten NutzerInnen schützen ihre Identität(en) nur unzureichend. Zwar können bestimmte technische Lösungen, die bereits heute einen verbesserten Schutz privater Daten bieten, auch in einer AmI-Welt einige der Sicherheitsprobleme reduzieren – gänzlich verschwinden werden diese primär durch sorgloses Nutzerverhalten erzeugten Schwachstellen indessen nicht.

Ausschnitt aus Szenario 2, welches den „menschlichen Faktor“ bei AmI-Anwendungen thematisiert:

> And thanks to the travel-assistance procedure of the AmI environment in our home in Murnau, this time we even thought of recharging our PWCs [personal wrist communicator] and HMDs [health monitoring device] early enough to avoid losing “our identity” like on our last trip. (Wright et al. 2008b, S. 73)

Stress aufgrund von Abhängigkeit

Massive Abhängigkeit von technischen Systemen kann Stress erzeugen. Sobald eine Technologie, die vollständig in das alltägliche Leben integriert ist, plötzlich nicht mehr zur Verfügung steht bzw. zeitweise ausfällt, werden gewohnte Abläufe und Routinen gestört. Stress entsteht insbesondere dann, wenn Unsicherheit darüber besteht, wann und ob überhaupt der ursprüngliche Zustand wiederhergestellt werden kann.
Ausschnitt aus Szenario 1:

> Paul receives an alarm signal on his PWC. There is an intruder in the house. “How is that possible?” he asks himself. He knows that his son Ricardo is home. He had invited some friends to play a new virtual reality game (for which Ricardo has a licence) from the entertainment centre downstairs. Paul checks the home surveillance system remotely but only gets a still image from 30 minutes ago. There is no live image available from the front and back door cameras, nor is Paul able to play back who has passed in front of the doors today. Ricardo does not answer his calls. “What’s happening? Where is he?” (Wright et al. 2008b, S. 36)

Falsche Verdächtigung

Aufgrund von fehlerhaften Datenprofilen können unschuldige Personen fälschlicherweise als Verdächtige oder potenzielle Sicherheitsrisiken identifiziert werden. Neben technischen Ursachen, die dafür verantwortlich sein können, erhöht sich die Wahrscheinlichkeit falscher Verdächtigungen insbesondere dann, wenn die Spannung zwischen öffentlichen Sicherheitsbedürfnissen und privaten Schutzrechten einseitig zugunsten der Ersteren aufgelöst wird. Zudem kann eine Kriminalisierung von Unschuldigen bereits durch unvollständige oder entkontextualisierte Datenprofile ausgelöst werden:
Ausschnitt aus Szenario 1:

> Paul is just leaving the office to return home when his boss calls, “Come in, Paul. I’m glad you are still at the office. It seems we have a small problem… I’ve just been contacted by the police who have asked for access to all the data we have on you. I understand this is just an informal request so we do not have to give them anything, but, as you know, as a security company, we cannot afford any suspicions of our staff.”
>
> Paul is astonished and does not understand what is happening. First the home problem, now this. “Surely, this must be some kind of mistake. I don’t know why they’d want my data – although I have heard lately of cases where the police have been investigating innocent people based on inadequate profiling. (Wright et al. 2008b, S. 36)

Kontrollverlust und bösartiger Angriff

Der Verlust der Kontrolle über bestimmte AmI-Anwendungen muss nicht zwingend auf den Voreinstellungen des Systems beruhen. Denkbar sind auch bösartige Angriffe durch

Unbefugte, die einen Kontrollverlust zur Folge haben können. Eine solche Situation wird ebenfalls in einem der Szenarien dargestellt. Nachdem die Hacker oder Angreifer die teilweise oder gar vollständige Kontrolle über das AmI-System erlangt haben, sind sie unter Umständen in der Lage, persönliche Profile zu verändern und/oder sensible Daten abzurufen, um diese für illegale Zwecke zu missbrauchen. Ausschnitt aus Szenario 1:

> Paul receives multiple messages on his PWC the moment he leaves his boss's office. He had all incoming communications on hold from the moment he entered her office. This is a company default setting. There is one message that immediately attracts his attention. "If you want your house systems to work again, click on the following link…" "What? I'm being blackmailed! So that's why I couldn't get access to my home systems, nor could the local security agent. That's why I got the intruder message," he thinks, slightly reassured, since that probably means that his children at home are OK. (Wright et al. 2008b, S. 37)

5 Schutzvorkehrungen für eine Welt mit intelligenten Umgebungen

Im Zuge der Analyse der dunklen Szenarien wurde eine Vielzahl potenzieller Risiken identifiziert, die durch künftige AmI-Anwendungen hervorgerufen werden können. Entsprechend dieser Vielfalt wird eine große Bandbreite unterschiedlicher Maßnahmen benötigt, um den Risiken angemessen zu begegnen. Die zu entwickelnden Schutzvorkehrungen, so die Erkenntnisse aus der Szenarien-Analyse, sollten möglichst ganzheitlich und zugleich kontextabhängig sein, um ökonomische, rechtliche, soziale, ethische und technische Aspekte abdecken zu können sowie die Interessen von Anbietern wie Nutzern zu berücksichtigen. Eine weitere Herausforderung besteht darin, die unterschiedlichen, oft in verschiedenen Politikfeldern angesiedelten Maßnahmen so aufeinander abzustimmen, dass sie den größtmöglichen Schutz entfalten und nicht intendierte Wirkungen – etwa die Exklusion von Nutzern aufgrund fehlerhafter Identitätsdaten – begrenzen. Zudem ist davon auszugehen, dass aufgrund des raschen technologischen Fortschritts und der korrespondierenden soziotechnischen Entwicklungen abgewandelte und zum Teil neue Risiken entstehen, was wiederum die kontinuierliche Anpassung der Schutzvorkehrungen erforderlich machen wird. Die im Rahmen von SWAMI vorgeschlagenen Schutzmaßnahmen fallen in drei Hauptkategorien: technische, organisatorische und rechtliche Vorkehrungen.

1. Die *technischen* Maßnahmen, die zum Schutz der Privatsphäre im Kontext von AmI beitragen sollen, basieren in aller Regel auf Anonymität, Pseudonymität und / oder Unverknüpfbarkeit verschiedener Datensätze. Grundsätzlich treten hierbei Konflikte auf zwischen dem Datensubjekt und den Anforderungen desjenigen, der die Daten sammelt und verarbeitet (vgl. Čas 2005; Vildjiounaite et al. 2008). Ein wichtiger Schutzmechanismus kann sich auf die Kontrolle der Datenzugangsprozeduren beziehen, die unaufdringlich und kontextabhängig sind sowie multimodale Authentifizierungsverfahren zur Verfügung stellen. Zudem können sichere Authentifizierungsmethoden, die auf Zero-knowledge-Techniken beruhen und einen minimalen Bedarf an Datenspeicherung vorsehen, dazu beitragen, die irrtümliche Protokollierung sensibler Daten zu vermeiden. Fortgeschrittene Techniken, die auf künstlicher Intelligenz basieren, können ferner Zugangskontrollen sicherer machen, indem ungewöhnliche Verhaltensmuster erkannt werden. Die öffentliche Forschungsförderung, so eine weitere Forderung von SWAMI, sollte künftig weitaus stärker die sicherheits- und datenschutzrelevanten Schlüsselthemen in F&E-Projekte integrieren.
2. Zu den *organisatorischen* Schutzmaßnahmen, die von SWAMI vorgeschlagen wurden, zählen u. a.: die Unterstützung offener Standards, um Interoperabilitätskonflikte zu minimieren; die breite Umsetzung von internationalen ISO-Standards im Bereich von Datenschutz und -sicherheit (z. B. ISO 17799); die Entwicklung und Verbreitung von datenschutzrechtlichen Qualitätssiegeln, um das Vertrauen in AmI-Dienste und -Infrastrukturen zu erhöhen; die Einführung von öffentlichen Reputationssystemen, um den Nutzern zusätzliche Orientierung über die Vertrauenswürdigkeit eines Anbieters zu geben. Eine wichtige Rolle bei der Verbreitung von Schutzvorkehrungen kann zudem ein entsprechendes Beschaffungsverhalten

der öffentlichen Hand spielen. Letztendlich bleibt auch hier ein wesentliches Ziel, die Kompetenz der Nutzer im Umgang mit AmI-Anwendungen zu steigern sowie das öffentliche Bewusstsein über potenzielle Gefahren für Datenschutz und -sicherheit zu erhöhen.

3. Die Analyse *rechtlicher* Regelungen hat aufgezeigt, dass bereits heute zahlreiche regulatorische und rechtliche Schutzvorkehrungen in Kraft sind, die auch in einem AmI-Kontext angewandt werden können. Zugleich ist aber deutlich geworden, dass AmI verschiedene neuartige rechtliche Fragen aufwirft – etwa, welchen Status Willenserklärungen haben, die im Namen des Nutzers im Rahmen eines automatisierten Identitätsmanagementverfahrens von technischen Assistenten abgegeben werden. Die Anpassung und Weiterentwicklung des gesetzlichen Rahmens sollte insbesondere Fragen des allgemeinen Zugangs und der Inklusion, der Zurechenbarkeit und der Haftung berücksichtigen.

Anmerkungen

1) Dieser Beitrag entstand im Rahmen des von der Europäischen Kommission geförderten Projekts SWAMI (IST-2004-006507). Er gibt die Meinung der Autoren wieder, die nicht notwendigerweise der Meinung der Europäischen Kommission entspricht.
2) Für einen genaueren Überblick über die Methodik vgl. Punie et al. 2006.
3) Die vollständigen Szenarien finden sich in Wright et al. 2008b, Kapitel 3 und Wright et al. 2008a.

Literatur

Aarts, E.; Appelo, L., 1999: Ambient Intelligence: thuisomgevingen van de toekomst. In: IT Monitor 9 (1999), S. 7-11

Čas, *J.*, 2005: Privacy in Pervasive Computing Environments – A Contradiction in Terms? In: IEEE Technology and Society Magazine 24/1 (2005), S. 24-33

Friedewald, M.; Lindner, R., 2007: Datenschutz, Privatsphäre und Identität in intelligenten Umgebungen: Eine Szenarioanalyse. In: Mattern, F. (Hg.): Die Informatisierung des Alltags: Leben in smarten Umgebungen. Berlin, Heidelberg, New York, S. 207-231

Gavigan, J.P., Scapolo, F.; Keenan, M. et al., 2001: A practical guide to Regional Foresight. Seville

Godet, M., 2000: The art of scenario and strategic planning: Tools and pitfalls. In: Technological Forecasting and Social Change 65/1 (2000), S. 3-22

ISTAG – IST Advisory Group et al., 2001: Scenarios for Ambient Intelligence in 2010. Luxembourg

Klinke, A.; Renn, O., 2001: Precautionary principle and discursive strategies: classifying and managing risks. In: Journal of Risk Research 4/2 (2001), S. 159-173

Masini, E.; Vasquez, J., 2000: Scenarios as Seen from a Human and Social Perspective. In: Technological Forecasting and Social Change 65/1 (2000), S. 49-66

Punie, Y., 2005: The Future of Ambient Intelligence in Europe: The Need for More Everyday Life. In: Communications and Strategies 57 (2005), S. 141-165

Punie, Y.; Maghiros, I.; Delaitre, S., 2006: Dark scenarios as a constructive tool for future-oriented technology analysis: Safeguards in a world of ambient Intelligence. Proceedings of the Second International Seville Seminar on Future-Oriented Technology Analysis: Impact of FTA Approaches on Policy and Decision-Making, Seville, 28-29 September 2006

Renn, O.; Zwick, M.M., 1997: Risiko- und Technikakzeptanz. Heidelberg und Berlin

Ringland, G., 1998: Scenario Planning. Managing for the Future. Chichester

van 't Klooster, S.A.; van Asselt, M.B.A., 2006: Practising the scenario-axes technique. In: Futures 38/1 (2006), S. 15-30

Vildjiounaite, E.; Rantakokko, T.; Alahuhta, P. et al., 2008: Privacy Threats in Emerging Ubicomp Applications: Analysis and Safeguarding. In: Mostéfaoui, S.K.; Maamar, Z.; Giaglis, G.M. (Hg.): Advances in Ubiquitous Computing: Future Paradigms and Directions. Hershey, PA, S. 320-351

Weiser, M., 1991: The Computer for the 21st Century. In: Scientific American 265/3 (1991), S. 94-104

Wright, D.; Friedewald, M.; Schreurs, W. et al., 2008a: The illusion of security. In: Communications of the ACM 51/3 (2008), S. 56-63

Wright, D.; Gutwirth, S.; Friedewald, M. et al. (Hg.), 2008b: Safeguards in a World of Ambient Intelligence. Dordrecht

Kontakt

Dr. Michael Friedewald
FhG-ISI, Karlsruhe
E-Mai: Michael.friedewald@isi.fraunhofer.de

« »