Safeguards in a World of Ambient Intelligence

The International Library of Ethics, Law and Technology

VOLUME 1

For other titles published in this series, go to
www.springer.com/series/7761

David Wright • Serge Gutwirth
Michael Friedewald • Elena Vildjiounaite
Yves Punie
Editors and Authors

Safeguards in a World of Ambient Intelligence

Pasi Ahonen • Petteri Alahuhta
Barbara Daskala • Sabine Delaitre
Paul De Hert • Ralf Lindner
Ioannis Maghiros • Anna Moscibroda
Wim Schreurs • Michiel Verlinden
Authors

Springer

David Wright
Trilateral Research & Consulting
London, UK

Serge Gutwirth
Vrije Universiteit Brussel
Belgium

Michael Friedewald
Fraunhofer Institute
for Systems and Innovation
Research (ISI)
Karlsruhe, Germany

Elena Vildjiounaite
VTT Technical Research Centre of Finland, Oulu
Finland

Yves Punie
Institute for Prospective
Technological Studies (IPTS)
European Commission JRC
Seville, Spain

ISSN 1875-0044
ISBN 978-1-4020-6661-0 (hardcover)
ISBN 978-90-481-8786-7 (softcover)
DOI 10.1007/978-1-4020-6662-7
Springer Dordrecht Heidelberg London New York

e-ISSN 1875-0036
e-ISBN 978-1-4020-6662-7

Library of Congress Control Number: 2010924814

Foreword by Emile Aarts

On the morning of 22 March 2006, I was hurrying to get to Brussels in time because I had to go there to present one of my Ambient Intelligence lectures. I was invited to give a keynote at an international conference with the name SWAMI, which was organized among others by the European Commission. I did not take the effort to study the scope of the conference in detail, nor did I take the time to have a close look at the list of participants. It had something to do with ethics I was told and I took it for granted that I could present my normal introductory ambient intelligence story. So I went to Brussels and I had a unique learning experience.

When I arrived at the conference hotel, they just had a break and I had to present just after the break. I started off with my normal positive and technology-driven motivation for the need to have ambient intelligence, but I could read from the faces of the audience that they were not amused by my argumentation. So I concluded that obviously this was all common knowledge to them and I started adding more industrial evidence for the economic value of ambient intelligence by reasoning about technology innovation and business models. This, however, resulted in even less positive feedback and faces grew darker, some persons in the audience even seemed to get annoyed by my presentation and evidently I had not found the right tone so far. So again I switched content and spoke a little about applications, but this also did not help. Then I remembered that the conference was about ethical things and I skipped to the last part of my presentation where I added a few slides with philosophical statements on the role of ambient intelligence in society, but harm was done already and this could hardly turn the presentation for the better.

I decided to stop and to open the floor for a discussion with the audience. One of the first remarks was a statement made by a nice person from Austria who exclaimed that my talk was "both ingenious and ridiculous". I will never forget this remark during my entire life and I assume that the gentleman intended to emphasize that he disliked the lack of social responsibility that I expressed in my talk, and he was right. For more than half an hour, we elaborated on these social implications in a plenary setting until the chairman stopped the discussion for the sake of time. The discussions went on for another hour in the hotel corridors and after that I had to leave for another meeting, almost an hour behind schedule, but chastened.

It is my true conviction that the work this group of persons had been doing is of utmost importance. The development of ambient intelligence is going on for almost

10 years now and most of the time we have been emphasizing the technological potential of this novel and disruptive approach. We also have been largely building on the belief that user insights and user-centric design approaches should be used to come up with solutions that really matter to people, but we hardly paid attention to questions related to such important matters as trust, security, and legal aspects, nor to speak about the more ethical issues such as alienation, digital divide, and social responsibility as raised and discussed by the SWAMI community.

This book, which can be viewed as a direct outcome of the 2006 SWAMI conference, presents a very comprehensive overview of all the relevant issues and options related to the ethics of ambient intelligence. The many high-quality contributions reflect the scholarship and integrity of its authors, and some of the chapters even resemble the level of a philosophical treatise. The book approaches ambient intelligence from a unique angle and it is mandatory reading material for anyone who is professionally active in the field of ambient intelligence as it can be seen as a landmark contribution to the discussion on ambient intelligence. After almost 10 years of development, ambient intelligence can now live up to its expectation that it can change peoples' lives for the better through its novel user-centric technology. In the end, however, this will only work if we can settle the ethical issues that are connected to it, and the SWAMI effort has contributed significantly to this greater cause.

Finally, I would like to thank the SWAMI people for giving me the opportunity to have one of the most compelling learning experiences in my professional life.

Emile Aarts
Scientific Program Manager
Philips Research
Eindhoven, The Netherlands
2 February 2007

Foreword by Gary T. Marx

SWAMI, How I Love Ya

For I dipt into the future, far as human eyes could see,
saw the world, and all the wonders that would be

Alfred Lord Tennyson, "Locksley Hall"

And you will have a window in your head.
Not even your future will be a mystery
Any more. Your mind will be punched in a card
And shut away in a little drawer.
When they want you to buy something
They will call you....
So friends, every day do something
That won't compute....

Wendell Berry, "The Mad Farmer Liberation Front"

These poems reflect polar images of science and technology in western societies. Such contrasting views are daily expressed in our literature, popular culture, politics, policies and everyday life. We are enthralled by, and fearful of, the astounding powers new technologies may bring. We hope with Edison that "whatever the mind of man creates" can be "controlled by man's character", even as we worry with Einstein that technological progress can become "like an axe in the hand of a pathological criminal".

In our dynamic and very unequal worlds of such vast system complexity, there is much to be worried about. But there is also much to be optimistic about. This book is a welcome contrast to much of the disingenuous commentary on new information technologies offered by technical, commercial and political advocates who command the largest megaphones. The book strikes a balance between encouraging the wonders that could be, while reminding us of the dark forces of history and society, and that nature is filled with surprises. We cannot and should not stop invention, but neither should we uncritically apply it, absent the careful controls and continual evaluation the book recommends.

Before our age of avaricious, data-hungry sensors that can record everything in their path, to say that a person "really left a mark" implied that they willfully did

something special. Now, merely being passively present – whether in a physical or biological sense, let alone actively communicating, moving or consuming leaves remnants as well. In an age when everyone (and many objects) will continuously leave marks of all sorts, that phrase may become less meaningful.

The topic of this book is ostensibly the embedding of low visibility, networked sensors within and across ever more environments (called ambient intelligence or AmI in Europe and ubiquitous computing or networked computing in America and Japan). But the book is about much more. It offers a way of broadly thinking about information-related technical developments. It is the most informative and comprehensive policy analysis of new information and surveillance technologies seen in recent decades.

Those wishing to praise a book often say, "*essential* reading for anyone concerned with …". But I would go beyond that strong endorsement to say *Safeguards in a World of Ambient Intelligence* (SWAMI) should be *required* reading for anyone concerned with public policy involving new communications and surveillance technologies. This should be bolstered by frequent certifying quizzes (and maybe even licenses) for those developing and applying information technology and for those on whom it is applied. The goal is to keep ever in view the multiplicity of analytical factors required to reach judgments about technologies which so radically break with the limits of the human senses and of space and time. In encouraging caution and steps to avoid worst-case scenarios, such analysis can limit unwanted surprises occurring as a result of interactions within very complex networked systems.

How do I like this book? Let me count the ways. If this were a musical comedy, the first song would be "SWAMI, How I love Ya, How I love ya" (with apologies to George Gershwin). First, it creatively and fairly wends its way through the minefields of praise and criticism that so inform our contradictory views of technology. It avoids the extremes of technophilia and technophobia implied in the poems above and often in superficial media depictions and in rhetorical excesses of the players. It also avoids the shoals of technological, as against social and cultural, determinism. There is nothing inherent in technology or nature that means specific tools must be developed or used. The social and cultural context is central to the kind of tools developed and their uses and meaning. Yet technologies are rarely neutral in their impact. They create as well as respond to social and cultural conditions.

The book suggests a flashing yellow light calling for caution and analysis rather than the certainty of a green or a red light. This can be seen as a limited optimism or a qualified pessimism, but what matters is the call for humility and continual analysis. As with much science fiction, the dark scenarios the book offers extrapolate rather than predict. They call attention to things that could happen in the hope that they would not.

While the report is a product of 35 experts, numerous meetings, work teams and consultants, it does not read like the typical pastiche committee or team report. Rather it is smooth flowing, consistent and integrated. The product of specialists from many parts of Europe, it nonetheless offers a common view of the issues that transcend the particularities of given cultures and language. As such, it speaks to an emerging European, and perhaps global, sense of citizenship fostered by standard-

ized technologies that so effortlessly transcend traditional national borders, as well as those of distance and time.

While the United States is the major player in the development and diffusion of new information technologies, it sadly lags far behind Europe in providing deep and comprehensive analysis of the social and ethical consequences of such technology. Not only does it lack privacy and information commissions, but there is no longer a strong national analytical agency concerned with the impact of new technologies. The short-sighted Congressional elimination of the nonpartisan analytical Office of Technology Assessment in 1995 has deprived the United States of an independent public interest voice in these matters.[1]

The book offers a very comprehensive review of the relevant literature from many fields, at least for the English language. As a historical record and chronicle of turn-of-the-century debates and concerns raised by these developments, the book will be of inestimable value to future scholars confronting the novel challenges brought by the continuing cascade of new information technologies. I particularly appreciate some of the metaphors and concepts the book uses such as data laundering, AmI technosis, technology paternalism, coincidence of circumstances, digital hermits, and the bubble of digital territory in its analysis.

Much of the extensive supporting documentation and reference material is available online, making it easy and inviting for the reader to pursue topics in more detail or to check on the book's interpretations. However, I hope this would not soon come with an AmI program that, seeing what was accessed, makes recommendations for future reading or offers discounts for related book purchases or worse sends political messages seeking to alter the assumed positions of the user/reader.

The strength of this book is in raising basic questions and offering ways of thinking about these. Answers will vary depending on the context and time, but the social factors and trade-offs that must be considered remain relatively constant. Rules and regulations will differ depending on the setting and the phase. A given use can be approached through a temporal process as we move from the conditions of collection to those of security and use. Or settings can be contrasted with respect to issues such as whether individuals should be given maximum, as against no, choice regarding the offering/taking of their personal data; questions around the retention or destruction of personal information; and whether the data should be seen as the private property of those who collect it, those about whom it is collected, or as a public record. A related issue involves whether AmI systems are viewed as public utilities in principle available to all or are viewed as private commodities available only to those who can afford them and/or who qualify.

---

[1] In a blatantly partisan and socially destructive move, the 104th Congress withdrew funding for OTA and its full-time staff of 143 persons. Copies of OTA publications are available from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7974. As this book notes, the National Research Council has stepped in to partially fill the void, most recently with the Committee on Privacy in the Information Age, *Engaging Privacy and Information Technology in a Digital Age*, 2007.

It has verisimilitude both in its treatment of the policy issues and in its scenarios. It offers an encyclopedia of safeguards and calls for a mixture of available means of regulation. While the book gives appropriate attention to technical controls and those involving legislation and courts at many levels (national, European community, international) and notes the role of markets, it stands apart from the voluminous policy literature in attending to civil society factors such as the media, public awareness and education, cultural safeguards and emerging tools such as trust marks, trust seals and reputation systems. The informal, as well as the formal, must be part of any policy considerations and analysis of impact.

An aspect of the book's reality check is its consideration of the trade-offs and tensions between conflicting goals and needs. In spite of the promises of politicians and marketeers and the fantasies of children, we cannot have it all. Hard choices must often be made and compromises sought.

In the rush to certainty and in the pursuit of self-interest, too much discussion of technology shows a misguided *either/or* fallacy. But when complex and complicated topics are present, it is well, with Whitehead, not to find clarity and consistency at the cost of "overlooking the subtleties of truth". We need to find ways of reconciling, both intellectually and practically, seemingly contradictory factors.

In considering issues of computers and society, there are enduring value conflicts and ironic, conflicting needs, goals and consequences that require the informed seeking out of the trade-offs and continual evaluation the book recommends.

These can be considered very abstractly as with the importance of liberty and order, individualism and community, efficiency and fair and valid treatment. When we turn to AmI, we see the tensions more concretely.

Thus, the need for collecting, merging and storing detailed personal information in real time, on a continual basis across diverse interoperable systems, is central for maximizing the potential of the AmI. But this can cause tension between the goals of authentication, personalized service and validity and those of privacy and security (the latter two can, of course, also be in tension, as well as mutually supportive). The generation of enormous databases presents monumental challenges in guarding against the trust-violations of insiders and the damage that can be wrought by outsider hackers. How can the advantages of both opacity and transparency be combined such that systems are easy to use and in the background and hence more egalitarian and efficient, while simultaneously minimizing misuse and encouraging accountability and privacy? As the song says, "something's got to give". Personalization with its appreciation of the individual's unique needs and circumstances must be creatively blended with impersonalization with its protections of privacy and against manipulation. We need solutions that optimize rather than maximize with a keen awareness of what is gained and what is lost (and for whom under what conditions) with different technical arrangements and policy regimes.

Under dynamic conditions, the balance and effort to mange competing needs must be continuously revisited. Some changes are purposive as individuals and organizations seek to undermine AmI as its operation becomes understood, others involve growth and development as individuals change their preferences and behavior, and environmental conditions change.

The dark scenarios are particularly refreshing given the predominance of good news advocacy stories in our culture. The bad news stories offered here are hardly the product of an unrestrained dystopian imagination rambling under the influence of some banned (or not yet banned) drug. Rather, they reflect a systematic method relying on cross-observer validation (or more accurately review and certification). This method should be in the toolkit of all analysts of new technology. Unlike the darkness of much science fiction, these stories are reality-based. The methodology developed here involves both a technology check (are the technologies in the stories realistic given current and emerging knowledge and technique?) and an actuality check (have the outcomes to some degree actually occurred, if not all at the same time or in exactly the same way as the story describes?).

These restrictions give the scenarios plausibility absent in fiction bounded only by the imagination of an author. However, for some observers, requiring that similar events have actually happened might be seen as too stringent. For example, by these standards the Exxon oil spill (prior to its occurrence) could not have been a scenario. This is because something like it had never happened and the chance of it happening was so wildly remote (requiring the coming together of a series of highly improbable events), that it would have been deemed unrealistic given the above methodology.

An extension or reversal of George Orwell?

The aura of George Orwell lies behind many of the critical concerns this book notes. In some of its worst forms (being invisible, manipulative and exclusionary, not offering choice, furthering inequality and ignoring individuality and individual justice in pursuit of rationality and efficiency across many cases), ambient intelligence reflects *1984*. It could even bring horrors beyond Orwell where surveillance was episodic, rather than continual, and relied on fear, lacking the scale, omnipresence, depth, automatism and power of ambient intelligence. With the soft and unseen dictatorship of design, the individual could face ever fewer choices (e.g., being unable to pay with cash or using an anonymous pay telephone) and if able to opt out and do without the benefits, becomes suspicious or at least is seen as someone who is socially backward as a result of nonparticipation. Rather than mass treatment which, given its generality, left wiggle room for resistance, the new forms drawing on highly detailed individuated information could greatly enhance control.

Orwell's treatment of language can be applied. With "Newspeak" and phrases such as "peace is war", Orwell's satire emphasizes how concepts can euphemize (or maybe euthanize would be a better term) meaning. To call this book's topic "ambient intelligence" brings a positive connotation of something neutral and supportive in the background, maybe even something warm and fuzzy. Ambience is popularly used to refer to a desired environmental condition. Like surround sound, it envelops us, but unlike the latter, we may be less aware of it. Ambient has been used as the name of a popular pill that induces somnolence. What feelings would be induced if the book's topic was instead called "octopus intelligence" or, given a record of major failures, "hegemonic stupidity"?

But there are major differences as well. In Orwell's Oceania, the centralized state is all-powerful and the citizen has neither rights nor inputs into government. Mass communication is rigidly controlled by, and restricted to, the state. There are no voluntary associations (all such organizations are directly sponsored and controlled by the state). The standard of living is declining and all surplus goes into war preparation rather than consumption. Society is hierarchically organized, but there is little differentiation, diversity or variety. Everything possible is standardized and regimented. Individuals are isolated from, and do not trust, each other. Private communication is discouraged and writing instruments are prohibited, as are learning a foreign language and contact with foreigners.

Yet empirical data on communications and social participation for contemporary democratic societies does not generally reflect that vision, even given the restrictions and enhanced government powers seen since 9/11. Indeed in its happier version, ambient intelligence can be seen as the antidote to a 1984-type of society – networked computers relying on feedback going in many directions can bring decentralization and strengthen horizontal civil society ties across traditional borders. Differences – whether based on space and time or culture – that have traditionally separated persons may be overcome. The new means vastly extend and improve communication and can offer informed end-users choices about whether or not, or to what degree, to participate. Pseudonymous means can protect identity. In the face of standardized mass treatment, citizens can efficiently and inexpensively be offered highly personalized consumer goods and services tailored to their unique needs.

The potential to counter and avoid government can protect liberty. On the other hand, privatization can bring other costs including insulation from regulation in the public interest and increased inequality. Those with the resources who do not need the advantages the technology offers in return for the risks it brings may be able to opt out of it. Those with the right profiles and with the resources to participate, or to pay for added levels of security, validity and privacy for their data, will benefit, but not others.

In many ways, we have moved very far from the kind of society Orwell envisioned in 1948. His book remains a powerful and provocative statement for a 19th-century kind of guy who never rode on an airplane and did not write about computers. Yet, if forced to choose, I would worry more (or at least as much) about the threat of a crazily complex, out-of-control, interventionist society that believes it can solve all problems and is prone to the errors and opaqueness envisioned by Kafka than about Orwell's mid-20th-century form of totalitarianism. Hubris was hardly a Greek invention.

While there is societal awareness of mal-intentioned individuals and groups to the extent that "Orwellian" has become clichéd, yet the threat posed by rushing to technologically control evermore aspects of highly complex life through constant data collection and feedback, interaction and automated actions is less appreciated and understood. The emergent dynamism of the involved interdependent systems and the difficulty of imagining all possible consequences must give us great pause.

The book's scenarios offer a cornucopia of what can go wrong. Ideally, we wish to see well-motivated people and organizations using good and appropriate technology. The book's dark scenarios suggest two other forms to be avoided:

Bad or incompetent people and/or organizations with good technology. The problem is not with the technology, but with the uses to which it is put. There may be an absence of adequate regulation or enforcement of standards. Individuals may lack the competence to apply the technology or end users may not take adequate protection and may be too trusting. As with identity theft, the wrongful cleansing and misuse of legitimately collected data, and machines that are inhuman in multiple ways, malevolent motivation combined with powerful technologies is the stuff of our worst totalitarian nightmares. But consider also the reverse:

Good people and/or organizations with bad or inappropriate technology. This suggests a very different order of problem – not the absence of good will, competence and/or legitimate goals, but of technology that is not up to the job and spiraling expectations. Achieving the interoperability and harmonization among highly varied technical and cultural systems that AmI networks will increasingly depend on can bring new vulnerabilities and problems. For technical, resource or political reasons, many systems will be incompatible and varying rates of changes in systems will affect their ability to co-operate. Technology that works in some settings may not work in others or may be neutralized in conflict settings. Here we also see the issue of "natural" errors or accidents that flow from the complexity of some systems and the inability to imagine outcomes from the far-flung interactions of diverse systems. Regular reading of the *Risks Digest* (http://www.csl.sri.com/~risko/risks.txt) can not only give nightmares, but also make getting out of bed each day an act of supreme courage.

From one standpoint, there are two problems with the new communication and information technologies. The first is that they do not work. The second is that they do. In the first case, we may waste resources, reduce trust, damage credibility and legitimacy and harm individuals. Yet, if they do work, we risk creating a more efficient and mechanical society at the cost of traditional human concerns involving individual uniqueness and will. Given power and resource differentials, we may create an even more unequal society further marginalizing and restricting those lacking the resources to participate and/or to challenge technical outcomes. There will be new grounds for exclusion and a softening of the meaning of choice. The failure to provide a detailed profile, or of a country to meet international standards, may de facto mean exclusion.

The book notes the importance of (p. xxvi) "focusing on concrete technologies rather than trying to produce general measures". Yet, in generating specific responses, we need to be guided by broad questions and values and the overarching themes the book identifies. These change much more slowly, if at all, than the technologies. That is of course part of the problem. But it can also be part of the solution in offering an anchoring in fundamental and enduring human concerns.

An approach I find useful amidst the rapidity and constancy of technical innovation is to ask a standard set of questions. This gives us a comparative framework for judgment. The questions in Table 1 incorporate much of what this book asks us to consider.[2]

A central point of this book is to call attention to the contextual nature of behavior. Certainly these questions and the principles implied in them are not of equal weight, and their applicability will vary across time periods depending on need and perceptions of crisis and across contexts (e.g., public order, health and welfare, criminal and national security, commercial transactions, private individuals, families, and the defenseless and dependent) and particular situations within these. Yet, common sense and common decency argue for considering them.

Public policy is shaped by manners, organizational policies, regulations and laws. These draw on a number of background value principles and tacit assumptions about the empirical world that need to be analyzed. Whatever action is taken, there are likely costs, gains and trade-offs. At best, we can hope to find a compass rather than a map and a moving equilibrium instead of a fixed point for decision making.

For AmI, as with any value-conflicted and varied-consequence behavior, particularly those that involve conflicting rights and needs, it is essential to keep the tensions ever in mind and to avoid complacency. Occasionally, when wending through competing values, the absolutist, no-compromise, don't-cross-this-personal line or always-cross-it standard is appropriate. But, more often, compromise (if rarely a simplistic perfect balance) is required. When privacy and civil liberties are negatively affected, it is vital to acknowledge, rather than to deny this, as is so often the case. Such honesty can make for better-informed decisions and also serves an educational function.

These tensions are a central theme in this book, which calls for fairly responding to (although not necessarily equal balancing of) the interests of all stakeholders. Yet, it only implicitly deals with the significant power imbalances between groups that work against this. But relative to most such reports, its attention to social divisions that may be unwisely and unfairly exacerbated by the technology is most welcome.

In a few places, the book lapses into an optimism (perhaps acceptable if seen as a hope rather than an empirical statement) that conflicts with its dominant tone of complexity and attention to factors that should restrict unleashing the tools.

---

[2] Adapted from G.T. Marx, "Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies", *Law and Social Inquiry*, Vol. 30, No. 2, 2005. A related factor is to identify the background assumptions and tacit empirical and moral beliefs that underlie attitudes toward technology. In a presentation to the 2006 SWAMI conference in Brussels where various parts of this book were presented, I identified 38 such beliefs. Perhaps the most important is not confusing data with knowledge, nor technique with wisdom. "Rocky Bottoms: Techno-Fallacies of an Age of Information", *International Political Sociology*, Vol. 1, No. 2, 2007. In G.T. Marx and G. Muschert, "Personal Information, Borders, and the New Surveillance Studies", *Annual Review of Law and Social Science*, Vol. 3, 2007, we discuss value conflicts and ironic and conflicting needs, goals and consequences. These and other related articles are at garymarx.net and G.T. Marx, *Windows Into the Soul Surveillance and Society in an Age of High Technology,* University of Chicago Press, forthcoming.

Table 1 Questions for judgment and policy

1. *Goals* – Have the goals been clearly stated, justified and prioritized? Are they consistent with the values of a democratic society?
2. *Accountable, public and participatory policy development* – Has the decision to apply the technique been developed through an open process and, if appropriate, with participation of those to be subject to it? This involves a transparency principle.
3. *Law and ethics* – Are the means and ends not only legal, but also ethical?
4. *Opening doors* – Has adequate thought been given to precedent creation and long-term consequences?
5. *Golden rule* – Would the controllers of the system be comfortable in being its subject, as well as its agent? Where there is a clear division between agents and subjects, is reciprocity or equivalence possible and appropriate?
6. *Informed consent* – Are participants fully apprised of the system's presence and the conditions under which it operates? Is consent genuine (i.e., beyond deception or unreasonable seduction or denial of fundamental services) and can "participation" be refused without dire consequences for the person?
7. *Truth in use* – Where personal and private information is involved does a principle of "unitary usage" apply, whereby information collected for one purpose is not used for another? Are the announced goals the real goals?
8. *Means–ends relationships* – Are the means clearly related to the end sought and proportional in costs and benefits to the goals?
9. *Can science save us?* – Can a strong empirical and logical case be made that a means will in fact have the broad positive consequences its advocates claim (the does-it-really-work question)?
10. *Competent application* – Even if in theory it works, does the system (or operative) using it apply it as intended and in the appropriate manner?
11. *Human review* – Are automated results with significant implications for life chances subject to human review before action is taken?
12. *Minimization* – If risks and harm are associated with the tactic, is it applied to minimize these showing only the degree of intrusiveness and invasiveness that is absolutely necessary?
13. *Alternatives* – Are alternative solutions available that would meet the same ends with lesser costs and greater benefits (using a variety of measures not just financial)?
14. *Inaction as action* – Has consideration been given to the "sometimes it is better to do nothing" principle?
15. *Periodic review* – Are there regular efforts to test the system's vulnerability, effectiveness and fairness and to review policies and procedures?
16. *Discovery and rectification of mistakes, errors and abuses* – Are there clear means for identifying and fixing these (and in the case of abuse, applying sanctions)?
17. *Right of inspection* – Can individuals see and challenge their own records?
18. *Reversibility* – If evidence suggests that the costs outweigh the benefits, how easily can the means (e.g., extent of capital expenditures and available alternatives) be given up?
19. *Unintended consequences* – Has adequate consideration been given to undesirable consequences, including possible harm to agents, subjects and third parties? Can harm be easily discovered and compensated for?
20. *Data protection and security* – Can agents protect the information they collect? Do they follow standard data protection and information rights as expressed in documents such as the Code of Fair Information Protection Practices and the expanded European Data Protection Directive?

This book (p. 8) sets for itself the "difficult task of raising awareness about threats and vulnerabilities and in promoting safeguards *while not undermining the efforts to deploy AmI*" and it suggests (p. 6) that "the *success* of ambient intelligence will depend on how secure its use can be made, how privacy and other rights of individuals can be protected, and, ultimately, how individuals can come to trust the intelligent world which surrounds them and through which they move". The book argues (p. xxii) that "matters of identity, privacy, security, trust and so on need to be addressed in a multidisciplinary way *in order for them to be enablers and not obstacles* for realizing ambient intelligence in Europe" (italics added).

Is the task of the public interest analyst to see that public policy involves "enablers not obstacles for realizing ambient intelligence in Europe"? Should the analyst try to bring about the future, guard against it (or at least prevent certain versions of it), or play a neutral role in simply indicating what the facts and issues are?

Certainly, where the voluntary co-operation of subjects is needed, the system must be trusted to deliver and to protect the security and privacy of valid personal information. Showing that people will be treated with dignity can be good for business and government in their efforts to apply new technologies. Yet, the book's call to implement the necessary safeguards will often undermine (if not prevent) "the efforts to deploy AmI".

Here, we must ask "what does success mean?" One answer: AmI is successful to the extent that the broad value concerns the book raises are central in the development of policy and practice. But another conflicting answer, and one held by many practitioners with an instrumental view, is that AmI is successful to the extent that it is implemented to maximize the technical potential and interests of those who control the technology. The incompatibility between these two views of success needs to be directly confronted.

Emile Aarts, who has played an important role in the development and spread of ambient intelligence, notes in the other foreword to this book that the technology's promise will "only work if we can settle the ethical issues that are connected to it". Yet, we must always ask just how well do we want it to work, what does "to work" mean, who does it work for and under what conditions? Furthermore, the day we *settle* the ethical and social issues we are in deep yogurt. Given the inherent conflicts and tradeoffs and dynamic and highly varied circumstances, we need to continually encounter and wrestle with unsettling and unsettled issues. This book offers us an ideal framework for that ongoing process.

Gary T. Marx
Professor Emeritus
Massachusetts Institute of Technology
Cambridge, MA, USA
http://www.garymarx.net
7 May 2007

Acknowledgements

We express special thanks to Laurent Beslay, who is now with the European Data Protection Supervisor (http://www.edps.europa.eu), for his initial contributions to our project. We also thank Marc Langheinrich of the Institute for Pervasive Computing at the Swiss Federal Institute of Technology, Zurich, Erkki Kemppainen of STAKES, Helsinki, and Jean-Marc Dinant, Head of the technology and security research unit in the Center for Research in Law and Computer Sciences (CRID) at the University of Namur for their excellent, independent review of our project deliverables.

We thank the following experts for their participation and useful comments at our workshops:

Achilles Kameas, Research Academic Computer Technology Institute, Patras, Greece
Albrecht Schmidt, University Duisburg Essen, Germany
Bart Walhout, Rathenau Instituut, The Hague, The Netherlands
Gregory Neven, KU Leuven, Belgium
Ian Brown, Foundation for Information Policy Research, London, UK
Irene Lopez de Vallejo, University College London, UK
Jan Möller, Federal Ministry of the Interior, Germany
Lorenz Hilty, Swiss Federal Materials Testing Agency, St. Gallen, Switzerland
Maddy Janse, Philips Research, Eindhoven, The Netherlands
Marc Langheinrich, ETH Zürich, Switzerland
Marco Conte, CE Consulting, Rome, Italy
Mario Hoffmann, Fraunhofer SIT, Darmstadt, Germany
Markus Hansen, Independent Data Protection Centre Schleswig-Holstein, Kiel, Germany
Michael Lyons, BTexact Technologies, Ipswich, UK
Michael Vanfleteren, Office of the European Data Protection Supervisor, Belgium
Miriam Lips, Tilburg University, The Netherlands
Norbert Streitz, Fraunhofer IPSI, Darmstadt, Germany
Pertti Huuskonen, Nokia Research Centre, Tampere, Finland
Sandro Bologna, Italian National Agency for New Technologies, Energy and the Environment, Rome, Italy

Spyros Lalis, University of Thessaly, Greece
Stefaan Seys, KU Leuven, Belgium

Finally, we acknowledge that although this book is based on a project funded by the European Commission, the views expressed herein are those of the authors alone and are in no way to be interpreted as those of the European Commission. We are grateful to our project officer, Inmaculada Placencia-Porrero, in the Directorate General for Information Society and Media, for her concurrence in the publication of this book.

Preface

This book is a warning. It aims to warn policy makers, industry, academia, civil society organisations, the media and the public about the threats and vulnerabilities facing our privacy, identity, trust, security and inclusion in the rapidly approaching future world of ambient intelligence (AmI).

The book has several objectives. First, as mentioned above, it aims to be a warning. Second, it aims to illustrate the threats and vulnerabilities by means of what we have termed "dark scenarios". Third, it sets out a structured methodology for analysing the four scenarios, and we believe that our methodology will serve others who seek to construct or deconstruct technology-oriented scenarios. Fourth, it identifies a range of safeguards aimed at minimising the foreseen threats and vulnerabilities. Fifth, it makes recommendations to policy-makers and other stakeholders about what they can do to ensure that we all benefit from ambient intelligence with the inevitable risks of negative consequences minimised as far as reasonably possible.

While we intentionally set out to display and illuminate the dark side of ambient intelligence in this book, we do not wish to be regarded as doomsayers or scaremongers, stridently opposed to AmI. We are as convinced of the social, political, economic and individual benefits of AmI as any of the enthusiasts. However, our enthusiasm is tempered by our concerns for the impacts on privacy, identity, security and so on. The threats and vulnerabilities can be minimised, if not eliminated. If AmI is to be a European success story, as it should be, we believe urgent action on a multiplicity of fronts is necessary. Delaying action until AmI is fully deployed will be too late.

The book grew out of the SWAMI project (Safeguards in a World of Ambient Intelligence), which began in February 2005 with funding from the European Commission under its Sixth Framework Programme of research and technological development. The SWAMI consortium comprises five partners, namely Fraunhofer Institute for Systems and Innovation Research (Germany), the VTT Technical Research Center of Finland, Vrije Universiteit Brussel (Belgium), the Institute for Prospective Technological Studies (IPTS, Spain) of the EC's Joint Research Centre, and Trilateral Research and Consulting (UK).

In addition to our co-authors, we offer our special thanks to Emile Aarts, Vice President of Philips, and Gary T. Marx, Professor at MIT, for agreeing to write the forewords for this book.

The editors

An Executive Summary for hasty readers

Ambient Intelligence (AmI) describes a vision of the future Information Society as the convergence of ubiquitous computing, ubiquitous communication and interfaces adapting to the user. In this vision, the emphasis is on greater user-friendliness, more efficient services support, user empowerment and support for human interactions. People are surrounded by intelligent intuitive interfaces embedded in all kinds of objects and an environment capable of recognising and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way.[1]

While most stakeholders paint the promise of AmI in sunny colours, there is a dark side to AmI as well. In a way, this dark side is inherent in many technologies including AmI, where intelligence is embedded in the environment and accessible anywhere and at any time including by those on the move. In this future, virtually every product and service – our clothes, money, appliances, the paint on our walls, the carpets on our floors, our cars, everything – will be embedded with intelligence. With networking microchips tinier than a pinhead, personalised services can be provided on a scale dwarfing anything hitherto available. Taken together, these developments will create a profoundly different information landscape from the one with which we are familiar today and that will have the following key characteristics[2]:

- *Complexity*: As hardware capabilities improve and costs reduce, there is continuing pressure to attempt to build systems of ever greater scope and functional sophistication.
- *Boundary-less nature of the systems and interconnectedness*: Few systems have a clear-cut boundary. They are subdivided into systems within systems.
- *Unpredictability*: All nodes, connected through a common infrastructure, are potentially accessible from anywhere at any time, which may result in unpredictable emergent behaviours.

---

[1] IST Advisory Group, K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten and J.-C. Burgelman, "Scenarios for Ambient Intelligence in 2010", Institute for Prospective Technological Studies (IPTS), EC-JRC, Seville, 2001; Punie, Y., "The Future of Ambient Intelligence in Europe: The Need for More Everyday Life", *Communications and Strategies* 57, 2005, pp. 141–165.

[2] Riguidel, M., and F. Martinelli, "Beyond the Horizon – Thematic Group 3: Security, Dependability and Trust", Report for Public Consultation, 2006. http://www.beyond-the-horizon.net

- *Heterogeneity and blurring of the human/device boundary*: For example, wearable and/or implantable devices will become more widely available and drop in cost.
- *Incremental development and deployment*: Systems are never finished; new features (and sources of system faults and vulnerabilities) are added at a continuous pace.
- *Self-configuration and adaptation*: Systems are expected to be able to respond to the changing circumstances of the ambient intelligence environment where they are embedded.

The scale, complexity and ever-expanding scope of human activity within this new ecosystem present enormous technical challenges for privacy, identity and security – mainly because of the enormous amount of behavioural, personal and even biological data (such as DNA, fingerprints and facial recognition) being recorded and disseminated. Moreover, many more activities in daily life, at work and in other environments, will depend on the availability of AmI devices and services. Questions of ownership and governance of infrastructures and services will thus loom large. The growing autonomy and intelligence of devices and applications will have implications for product liability, security and service definition. There will also be new and massive economic activity in the trading of those techniques that make things smart. One can expect vigorous discussions of who has rights over what information and for what purpose. Finally, there will be a constant struggle to defend this world of ambient intelligence against attacks from viruses, spam, fraud, masquerade, cyber terrorism and so forth. The risk of new vulnerabilities may prove to be one of the biggest brakes on the deployment and adoption of new capabilities and needs to be mitigated.[3]

This book considers how and to what extent it is possible or could be possible in the future to overcome the problematic implications of the dark side of ambient intelligence through the implementation of various safeguards and privacy-enhancing mechanisms, the aim of which is to ensure user control and enforceability of policy in an accessible manner and the protection of rights for all citizens in the Information Society.

There is an urgent need for realising these objectives. Matters of privacy, identity, trust, security and so on need to be addressed in a multidisciplinary way in order for them to become enablers and not obstacles for realising ambient intelligence in Europe. As often happens, technology is progressing faster than the policy-building process that might otherwise assuage public concerns about the potential for new encroachments on privacy and engender trust in our technological future.

These concerns are reflected in the four scenarios contained in this book. Scenarios are not traditional extrapolations from the present, but offer provocative glimpses of futures that can (but need not) be realised. Scenario planning provides a structured way to get an impression of the future and to uncover the specific steps and challenges in technology that have to be taken into account when anticipating the future. Most scenarios are developed so as to demonstrate the benefits of new technologies. By contrast, our scenarios are "dark" since they include applications that go wrong or do not work as expected. Our four scenarios are the following:

---

[3] Sharpe, B., S. Zaba and M. Ince, "Foresight Cyber Trust and Crime Prevention Project. Technology Forward Look: User Guide", Office of Science and Technology, London, 2004.

Dark scenario 1 (the AmI family) presents AmI vulnerabilities in the life of a typical family moving through different environments. It introduces dark situations in the smart home, at work and during a lunch break in a park.

Dark scenario 2 (a crash in AmI space) also references a family but focuses more specifically on senior citizens on a bus tour. An exploited vulnerability in the traffic system causes an accident, raising many different problems related to both travel and health AmI systems.

Dark scenario 3 (what is a data aggregator to do?) involves a data-aggregating company that becomes victim of theft of the personal data which it has compiled from AmI networks and which fuel its core business. Given its dominant position in the market, the company wants to cover this up but ends up in court two years later. The scenario draws attention to the digital divide between developed countries with AmI networks and developing countries that do not have such networks.

Dark scenario 4 (an early morning TV programme reports on AmI) portrays an AmI risk society from the studios of a morning news programme. It presents an action group against personalised profiling, the digital divide at a global scale and related to environmental concerns, the possible vulnerabilities of AmI-based traffic management systems and crowd control in an AmI environment.

The four scenarios deal with issues that need to be addressed for the successful deployment of ambient intelligence, among which are the following:

- **Privacy** – It is important to be aware of the implications of AmI for private life and personal data and to take adequate social, technical, economic and legal measures to protect privacy. The scenarios show different facets of privacy invasion, such as identity theft, the "little brother" phenomenon, data laundering, disclosure of personal data, surveillance and risks from personalised profiling.
- **Security** – This is a key challenge for successful AmI implementation. The scenarios depict security issues in different contexts: security imposed for telework, biometrics used for authentication or identification, human factors and security, malicious attacks, security audits, back-up security measures, security risks, access control, the illusion of security and viruses. The possible impacts that arise when there is a lack of security or unsuitable security measures are also underlined.
- **Identity** – The different components of identity, i.e., information related to legal identity, identification, authentication and preferences, play important roles in determining the feasibility of the AmI environment. The scenarios expose and detail the consequences when identity-based data are misused, erroneously used or incompletely processed.

- **Trust** – The notion of trust has technical aspects as well as social, cultural and legal aspects. In the scenarios, trust is raised in different connections: trust and confidence, lack of trust (from loss of control, unwillingness to provide some data, contextual misunderstandings) and honesty.
- **Loss of control** – This is one of the main issues in the dark scenarios and stems from different factors, for instance, when there is a lack of trust on the part of the citizen/consumer in the AmI infrastructure and its components. It can also emerge when the complexity level of AmI devices or services is too high and consequently does not enable users to get what they want. Strategies should be defined in order to compensate for the complexity and to weaken this feeling of loss of control.
- **Dependency** – This issue emerges directly from the usage of a technology by the user and the prospects (benefits and alternative solutions) for the technology. The scenarios mainly highlight its social impacts. Several situations are described, such as dependence on personalised filtering, on seamless and ubiquitous communications, on AmI systems (e.g., health monitoring and traffic management systems) and users' feeling of dependence and frustration when the technology does not work as expected.
- **Exclusion** (vs inclusion) – Exclusion may be voluntary, for instance, when a user switches off, but usually it is outside people's own will. The scenarios acknowledge that equal rights and opportunities for all need to be built into the design of new technologies since they are not achieved automatically. Exclusion can also be the result of lack of interoperability, denial of service, inadequate profiling and data mismatches.
- **Victimisation** – Citizens have a democratic right not to be treated as criminals (unless they are criminals, of course), otherwise, they will be unfairly victimised. The scenarios illustrate victimisation as an AmI impact by describing a disproportionate reaction based on unfounded suspicions and emphasise the difficulty in being able to act anonymously (anonymity is regarded as suspicious behaviour) and without being subject to anonymity profiling.
- **Surveillance** – Every citizen/consumer leaves electronic traces as the price of participation in the ambient intelligence society. These traces enable new and more comprehensive surveillance of our physical movements, use of electronic services and communication behaviour. These traces will make it possible to construct very sophisticated personal profiles and activity patterns. Although the justification for installing surveillance systems has a strong public interest dimension, i.e., for the safety and security of society, surveillance raises ethical, privacy and data protection issues. There is a clear need to delineate and define the boundaries between the private and public spheres.
- **Identity theft** – Without appropriate security, the AmI environment may provide malicious persons many opportunities to steal identity information and to use it for criminal purposes. The scenarios offer a picture of identity theft in AmI space and a new kind of crime, which is data laundering.
- **Malicious attacks** – Every new technology is plagued by known and/or unknown weaknesses, which threaten to serve as the backdoor for malicious

attackers. Some possible consequences and impacts are considered in the scenarios.

- **Digital divide** – AmI technology has the potential (because of its foreseen user friendliness and intuitive aspects) to bridge some aspects of the current digital divide but this same technology could also widen other aspects with regard to unequal access and use.
- **Spamming** – This encompasses several issues such as profiling, disclosure of personal data and malicious attacks.

In addition to the scenarios, this book presents an analytical approach we devised for both constructing and deconstructing the dark scenarios, but this approach, this methodological structure, could also be applied to many other technology-oriented scenarios. Our structured approach consists of several elements: the context describes the scenario situation (its purpose, a very brief resume), the technologies referenced in the scenario, the applications, the drivers (what factors impel the scenario), the issues raised, including a legal analysis of the issues, and our conclusions.

In addition to our scenario analysis *structure*, the book describes the *process* we followed to construct the scenarios. The process is depicted in Fig. 1.

Essentially, as shown in Fig. 1, we made an extensive review of existing AmI-related projects and studies, with particular reference to the scenarios. We held an experts workshop to discuss the most important threats and vulnerabilities posed by AmI. At an internal workshop, we brainstormed until we agreed the rough outlines of four contrasting scenarios. We then developed these outlines into scenario stories or scripts, and did a "technology check" (are the technologies referenced in the scenarios probable?) and a "reality check" (are there press reports of events similar to those mentioned in the scenarios?). Each of the partners reviewed all of

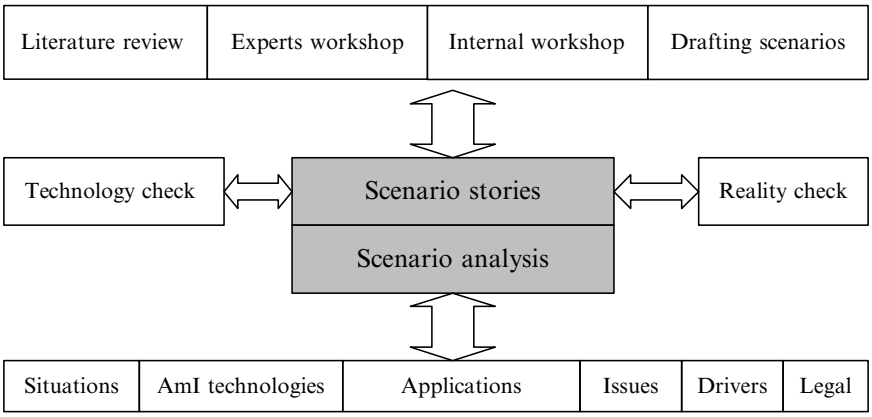

Fig. 1 The process of constructing the four dark scenarios

the scenarios in order to eliminate doubtful points, unnecessary wordage, irrelevancies, etc., and to sharpen them to illustrate the points we wanted to emphasise. Once the scenarios were "stable", we performed our analysis of them (following the structured approach as described above), the last part of which was the legal analysis, which was able to consider not only the scenarios, but also the analyses.

In addition to submitting our scenarios and analyses to the Commission, we presented the scenarios at a second workshop in order to benefit from the comments of other experts.

The scenarios and their analyses are followed by a chapter on threats and vulnerabilities and a chapter on safeguards, before arriving at the final chapter which contains our recommendations and conclusions, specifically addressed to the European Commission, Member States, industry, academia, civil society organisations and individuals. The main recommendations are these:

1. The European Commission and Member States, perhaps under the auspices of the European Network and Information Security Agency (ENISA), should initiate a formalised risk assessment/risk management process with regard to the risks posed by AmI to security and privacy. The assessment and decision-making process should be open, transparent and inclusive. Stakeholder groups should be identified and contacted and encouraged to take part in the process. Individuals should also be given an opportunity to express their views.
2. The Commission and Member States should invest in an awareness campaign specifically focused on AmI, the purpose of which would be to explain to all stakeholders, including the public, that AmI is on its way, that it offers great benefits, but also poses certain security and privacy challenges.
3. The Commission and Member States should review and address the inadequacies and lacunae in the existing legal and regulatory framework with respect to AmI.
4. Legal instruments should not prohibit new technological developments (even if it were possible to do so), but should "channel" them (such as by data protection and security measures). Focusing on concrete technologies rather than trying to produce general solutions seems to be more appropriate for AmI, an environment that adapts and responds to changes in context, and in which privacy and other legal issues are also context-dependent.
5. The Commission and Member States should be proactive in the development of a more comprehensive international co-operation framework that would take AmI technologies and capabilities into account as a matter of urgency.
6. The European Commission should ensure that projects that it funds take questions of privacy, security and trust into account. It should require project proposals to specifically speculate what privacy or security impacts might arise from their projects and what measures could be taken to address those. Member States should adopt a similar approach.

Sooner or later, we will live in an ambient intelligence type of world. For ambient intelligence to be a success story, in human terms, according to democratic principles, and not to be an Orwellian world, all stakeholders must be cognisant of the threats and vulnerabilities and work together to ensure that adequate safeguards exist.

Certainly, industry should become more active in creating applications that are secure and privacy enhancing since this is the major way to create consumer trust and make ambient intelligence fruitful to *all* participants. Industry should not view privacy, security, identity, trust and inclusion issues as regulatory barriers to be overcome. Rather, they should regard such measures as necessary, justified and, in the end, crucial to ensuring that their fellow citizens will use ambient intelligence technologies and services. In the meantime, we encourage all stakeholders to be vigilant.

Contents