Shining light on the dark side of ambient intelligence

David Wright is a Partner in Trilateral Research & Consulting, London, UK. Serge Gutwirth is a Professor of Law at the Vrije Universiteit Brussels (VUB), Belgium. Michael Friedewald is senior researcher and consultant at the Fraunhofer Institute for Systems and Innovation Research in Karlsruhe, Germany.

Purpose – *To identify safeguards against threats and vulnerabilities posed by the emerging world of ambient intelligence.*

Design/methodology/approach – *Dark scenarios were constructed to highlight the threats and vulnerabilities; safeguards are identified to address those threats and vulnerabilities and recommendations for specific stakeholders are made for implementing those safeguards.*

Findings – *A multiplicity of threats and vulnerabilities can be expected in the emerging world of ambient intelligence, and a multiplicity of safeguards are similarly necessary to address those.*

Research limitations/implications – *Additional technological research is necessary in order to develop some of the safeguards envisaged as necessary.*

Practical implications – *The existing legal and regulatory regime suffers from various lacunae and must be amended to address AmI challenges. Many stakeholders have important roles to play.*

Originality/value – *The paper identifies necessary safeguards to protect privacy, identity, trust, security and e-inclusion. It identifies specific recommendations for the European Commission, Member States, industry, civil society organizations, academia and individuals.*

Paper type *Viewpoint*

Introduction

In the European vision of ambient intelligence (AmI), the emphasis is on user friendliness, efficient services support, user empowerment and support for human interactions (ISTAG, 2003). People are surrounded by easy-to-use interfaces embedded in all kinds of objects and by an everyday environment capable of recognizing and responding to individuals in a seamless, unobtrusive and invisible way.

Realisation of the AmI vision, however, poses many political, social, economic, organizational and ethical challenges. Before ambient intelligence technologies do indeed become ubiquitous, our political decision-makers – indeed all stakeholders, including the public – need to consider options addressing:

- issues such as privacy, anonymity, manipulation and control, intellectual property rights, human identity, discrimination and environmental concerns;
- new societal responsibilities and the ethics of digital behavior;
- protection of rights for all citizens in all their roles (private and professional) in the Information Society;
- safeguards and privacy-enhancing mechanisms to ensure user control, user acceptance and enforceability of policy in an accessible manner; and

The views and opinions in this paper are those of the authors alone and in no way are intended to reflect those of the European Commission.

- equal rights and opportunities of accessibility to the Information Society and its ambient intelligence environment.

The definition of and provision for safeguards is critical for the rapid deployment and the further development of ambient intelligence in Europe. Instead of making people adapt to technology, we have to design technologies for people.

The European Commission, which has funded more AmI studies and projects than anyone else, has recognized that:

> . . . multidisciplinary research is needed on the social, legal, organisational and ethical issues associated with ambient intelligence, which places the individual at the centre of future developments for an inclusive knowledge based society for all. This includes also the investigation of the emerging challenges, in particular with respect to identity, privacy and protection of rights for all citizens in all their roles (private and professional) in the Information Society. It is important to identify new societal and policy options including responsibilities and ethics of digital behaviour. The task also requires research, on how to build into Information Society services and systems the safeguards and privacy enhancing mechanisms needed to ensure user control and enforceability of policy in an accessible manner (EC, 2003).

The SWAMI project, funded under the EC's Sixth Framework Programme, was created to examine these issues. SWAMI is the acronym for Safeguards in a World of Ambient Intelligence, which perfectly describes what the project was all about. More particularly, the consortium[1] had three objectives:

1. To identify the social, legal, organizational and ethical implications related to issues such as privacy, anonymity, manipulation and control, and identity in the context of ambient intelligence using current and future information and communications technologies.
2. To create and analyze four ''dark'' scenarios on AmI that highlight and detail the key socio-economic, legal, technological and ethical risks related to, in particular, identity, privacy and security.
3. To identify research and policy options on how to build into Information Society services and systems the safeguards and privacy enhancing mechanisms needed to ensure user control, user acceptance and enforceability of policy in an accessible manner, with a view to support accessibility and the provision of citizens with real equal rights and opportunities in a world of ambient intelligence.

At the outset of the project, in February 2005, the SWAMI partners began by reviewing well over 100 AmI-related projects in Europe, the United States and Japan to see to what extent the key issues of privacy, identity, trust, security and digital divide had been considered. Few projects had these issues as their prime focus, although some did flag these issues[2]. The second task of the SWAMI consortium was to prepare a set of ''dark'' scenarios as a means of highlighting the threats and vulnerabilities that we saw in ambient intelligence.

Dark scenarios

Most of the projects and studies examined by the SWAMI consortium were focused on the technical challenges of ambient intelligence, and most of the scenarios promoted the wonders of living in an AmI world. The SWAMI partners adopted a rather perspective and intentionally constructed four ''dark scenarios'', as we called them, a term coined to signify things that could go wrong in an AmI world, which were designed to expose some of the threats and vulnerabilities in AmI in the context of our key issues (privacy, identity, trust, security, digital divide).

The four scenarios, elaborated in the second SWAMI report, entitled *The dark side of ambient intelligence*, are the following:

1. *Dark scenario 1:* A typical family in different environments – 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 while taking a lunch break in a park.

2. *Dark scenario 2:* Seniors on a journey – 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.
3. *Dark scenario 3:* Corporate boardroom & court case – involves the Data Mining Corporation, an AmI data-aggregating company that becomes the victim of a theft of the personal AmI-generated data that 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 also highlights the disparities between countries with AmI networks and those without as well as the illusion of security.
4. *Dark scenario 4:* Risk society – From the studios of a morning news programme, this scenario portrays the AmI world as a risk society. It presents an action group against personalized profiling; the digital divide at a global scale and related to environmental concerns; the possible vulnerabilities of AmI traffic systems and crowd management.

The SWAMI partners devised a methodological structure for both constructing and deconstructing scenarios, not just the SWAMI scenarios, but many other technology-oriented scenarios. The SWAMI structure consists of the following elements:

Framing the scenario

This first step summarizes the scenario in question and explains its context – who are the main actors in the scenario, what happens to them or what they do, how far into the future is the scenario set, where it takes place and in what domain (home, office, on the move, shopping, etc). It identifies the type of scenario (trend, normative, explorative) and key assumptions (e.g. intelligent technologies will be embedded everywhere in rich countries, but not in poor countries).

Identifying the technologies and/or devices

Next, we identify the most important AmI technologies and/or devices used and/or implied in the scenarios.

Identifying the applications

We consider the applications that emerge in each scenario and that are supported by the technologies mentioned in the previous step.

The drivers

At this step in the analysis, we identify the key drivers that impel the scenario or, more particularly, the development and use of the applications. Drivers are typically socio-economic, political or environmental forces (e.g. the Data Mining Corporation seeks a global monopoly, economic disparities are inflaming poor countries, the world is becoming a hothouse) or personal motivations (e.g. greed).

Issues

Next, we identify and explicate the major issues raised by the scenario. In the SWAMI scenarios, the issues of concern, as mentioned above, are privacy, identity, trust, security and inclusiveness (or its opposite, the digital divide). A discussion of the issues considers the threats and vulnerabilities exposed by the scenario as well as their impacts and legal implications.

Conclusions

The final step is a reality check of the scenario itself (how likely is it? are the technologies plausible?) and a consideration of what should be done to address the issues it raises. One might conclude, as the SWAMI partners did, that a range of socio-economic, technological and legal safeguards are needed in order to minimize the risks posed by the threats and vulnerabilities highlighted by the scenario.

Threats and vulnerabilities

The SWAMI scenarios highlighted many of the threats and vulnerabilities that we foresee afflicting the AmI world. The principal difference (in our view) between an AmI world and that which we know today is the scale of the data that will be available. When everything is embedded with intelligence, when AmI is pervasive, invisible, ubiquitous, when everything is connected and linked (O'Harrow, 2005)[3], the threats and vulnerabilities that we know today will become even greater risks than they are now.

Privacy threats and vulnerabilities

In a world of ambient intelligence, the threats to our privacy multiply. In an AmI world, we can expect to be under surveillance (''transparent'') wherever we go because the permanent and real-time registration and processing of our presence and behavior is the precondition – the ''code'' – of ambient intelligence.

The threats to our privacy, however we define it, can come from many different sources. Here are some of the principal ones that affect us today and we can assume will still be threats in an AmI world. Many of these threats are also threats for identity and security:

- hackers and attackers;
- function creep, which occurs when data collected for one purpose are used for another;
- surveillance;
- profiling;
- lack of public awareness or concern about privacy rights;
- lack of enforcement and oversight of privacy rights;
- erosion of rights and values;
- uncertainties about what to protect and about the costs of protection;
- uncertainties about the economic costs of privacy erosion;
- lax security on our part or on the part of those who are supposed to be protecting our data; and
- government and industry are less than forthright about the personal data they collect and/or how they use that data.

Identity threats and vulnerabilities

Identity is associated with an individual as a convenient way to characterize that individual to others. The set of information and the identifier (name, label or sign) by which a person is known are sometimes referred to as that person's ''identity''. The choice of information may be arbitrary, linked to the purpose of the identity verification (authentication) in any given context, or linked intrinsically to the person, as in the case of biometrics.

Threats to our identity can come from various sources, among which are the following:

- identity theft;
- function creep;
- exploitation of linkages by industry and government;
- penetration of identity management systems (hacking, spoofing, denial of service, etc);
- authentication may intrude upon privacy;
- complexity of identity management systems;
- failures in identity management systems & authentication systems;
- people do not take adequate care to protect their cyber identity(-ies); and
- misplaced trust in security mechanisms.

Threats and vulnerabilities in trust

The issue of trust from the user's perspective would seem to merit greater consideration and more detailed study than heretofore has been the case. One of the most important inhibitors to public acceptance of the Internet for human interactions (commercial or otherwise) has been the lack of trust in the underlying cyber infrastructure and in other people whom we meet through that infrastructure.

SWAMI categorised threats to and vulnerabilities in trust in four areas: inadequate profiling, loss of control (which could be real or we believe we don't have control), service refusal and discrimination, and victimization. These areas are closely interrelated. For instance, poor profiling is a problem because the promised customization might be deficient and, at the same, because it represents a precondition for certain denials of services. Moreover, as the concept of trust is multi-dimensional, largely intangible and encompasses interdependent relationships, problems primarily related to privacy, identity, security and the digital divide are relevant for the issue of trust as well.

Security threats and vulnerabilities

The traditional taxonomy of security threats distinguishes between three main aspects in which threats may appear: confidentiality, integrity and availability (Stajano and Anderson, 2002). Confidentiality implies protection of information from unauthorized use, integrity implies protection of information from unauthorized modification, and availability implies that the system is capable of providing a service when users expect it. The protection properties all rely on the distinction between authorized and unauthorized entities. Protecting confidentiality, integrity and availability is more difficult in a ubiquitous computing environment than in traditional networks for the following reasons:

- possible conflict of interests between communicating entities;
- network convergence;
- large number of ad hoc communications;
- small size and autonomous mode of operation of devices; and
- resource constraints of mobile devices.

AmI will require security solutions very different from those of today's systems. ISTAG postulated what it called ''a new security paradigm'' characterized by ''conformable'' security in which the degree and nature of security associated with any particular type of action will change over time and circumstance.

Security threats and vulnerabilities fall into two major groups: malicious and unanticipated system behavior. Malicious system behavior can be caused by viruses, worms, Trojans, phishing, denial of service attacks or physical tampering. Unanticipated system behavior or failure is due to inadequate design, e.g. internal complexity and lack of user-friendliness.

Digital divide

Apart from the ISTAG scenarios, the digital divide issue has scarcely figured in any AmI-related projects, although the EC has initiated a significant eInclusion programme[4].

In general, it seems that AmI will narrow some gaps while widening existing or creating new ones at the same time. Physical access to AmI equipment and infrastructure is likely to improve, since AmI applications will form an intrinsic part of our every day lives and the basic infrastructure is bound to envelop the majority of the people. The AmI infrastructure will become cheaper and more affordable for larger parts of society (although it could also be argued that the network will be more complex, thus the cost higher for the providers). Furthermore, because of the envisioned user friendliness of AmI technology, the required skills and knowledge for its use will be less than that required today to use mobile phones, personal computers and the Internet, thus enabling more people to use its applications and receive the expected benefits. The majority of people are expected to be at least moderately computer literate, especially given the extent of use of technologies in everyday life.

On the other hand, there will still be a percentage of the population that will not have access to AmI applications and even a greater percentage that will have access only to basic infrastructure and not to more sophisticated devices, thus excluding them from accessing the full benefits of the AmI environment. Moreover, skills and knowledge remain a limiting factor. In a society with extreme levels of technology pervasiveness, people who do not possess the knowledge or the skills to use AmI will be more seriously excluded than today.

Serious concerns exist about the persistence of digital divides with regard to income, education and specific age groups, as well as gender and race / ethnicity. The global dimension of the digital divide between developed and developing countries is likely to remain the same or even grow. As long as the gap between developing and developed nations in general does not close, the digital divide will also widen, especially as new technologies emerge, which the under-developed societies do not have access to or cannot use. In effect, certain regions will most likely face the problem of accumulated digital divides.

Safeguards

The multiplicity of threats and vulnerabilities associated with AmI will require a multiplicity of safeguards to respond to the risks and problems posed by the emerging technological systems and their applications. In order to adequately address an identified threat or vulnerability, a combination of several safeguards might be needed; in other instances, a single safeguard has the potential to address numerous treats and vulnerabilities.

We grouped safeguards into three main approaches:

1. technological;
2. socio-economic; and
3. legal and regulatory.

Technological safeguards

The main privacy-protecting principles in network applications are:

- anonymity (possibility to use a resource or service without disclosure of user identity);
- pseudonymity (possibility to use a resource or service without disclosure of user identity, but still be accountable for that use);
- unlinkability (possibility to use multiple resources or services without others being able to discover that these resources were used by the same user); and
- unobservability (possibility to use a resource or service without others being able to observe that the resource is being used) (ISO, 1999).

The main difference between existing network applications and emerging AmI applications is two-fold: first, in the former case, the user has some understanding of which data about him are collected, and has some means to restrict data collection: e.g. to use a public computer anonymously to access certain web pages; to switch off his mobile phone, to pay cash instead of using a web service, etc. In the latter case, with the environment full of numerous invisible sensors (which might include video cameras), it is difficult, if not impossible, for users to understand and to control data collection and to achieve unobservability, anonymity and pseudonymity. Intelligent data processing, limiting linkability and implementing strong access control to collected data seem to be the main ways of protecting privacy in such applications. However, such applications present potential privacy threats anyway if the police, intelligence agencies, family members or criminals can search through devices that store personal data, or if the owner of the device discovers some interesting facts to which he has not paid attention while moving about or talking to people.

A second important difference between existing network applications and emerging AmI applications is that neither mobile devices nor web usage penetrates through such strong privacy protecting borders as walls (it is rarely 100 per cent certain who sends a request

from a particular IP address or uses a mobile device) and the human body, while physiological, video and audio sensors, proposed for AmI applications, will have much stronger capabilities to identify a person and to reveal personal activities and feelings.

Consequently, future AmI applications in smart environments will require stronger safeguards, many of which are not yet fully developed. In our third SWAMI report[5], we proposed research directions for developing privacy-protecting safeguards in future AmI settings, among which are the following:

- communication protocols which either do not require a unique device identifier at all or which require authorization for accessing the device identifier;
- network configurations that can hide the links between senders and receivers of data;
- improving access control methods by multimodal fusion, context-aware authentication and unobtrusive biometric modalities (especially behavioral biometrics, because they pose a smaller risk of identity theft) and by liveness detection in biometric sensors;
- enforcing legal requirements and personal privacy policies by representing them in machine-readable form and attaching these special expressions to personal data, so that they specify how data processing should be performed, allow a privacy audit and prevent any other way of processing;
- developing fast and intuitive means of detecting privacy threats, informing the user and configuring privacy policies;
- increasing hardware and software capabilities for real-time data processing in order to minimize the lifetime and amount of raw data in a system;
- developing user-friendly means to override any automatic settings in a fast and intuitive way;
- increasing security by detection of unusual patterns;
- increasing software intelligence by developing methods to detect and to hide sensitive data; to understand ethics and etiquette of different cultures; to understand and translate human speech in many languages, including a capability to communicate with the blind and deaf; and
- developing user-friendly means for recovery when security or privacy has been compromised.

Socio-economic safeguards

Co-operation between producers and users of AmI technology in all phases from R&D to deployment is essential to address some of the threats and vulnerabilities posed by AmI. The integration of or at least striking a fair balance between the interests of the public and private sectors will ensure more equity, interoperability and efficiency. Governments, industry associations, civil rights groups and other civil society organizations can play an important role in balancing these interests for the benefit of all affected groups.

Among the socio-economic safeguards we propose are those involving:

- standards, such as ISO 15408 and ISO 17799 on IT privacy and security respectively;
- privacy audits;
- codes of practice;
- trust marks and trust seals;
- reputation systems and trust-enhancing mechanisms;
- service contracts with strong privacy protections;
- guidelines for ICT research;
- emphasis on security and trustworthiness in public procurement;
- accessibility and social inclusion;

- raising public awareness;
- including privacy, identity and security issues in the professional education curriculum of computer scientists; and
- media attention, bad publicity and public opinion.

Legal and regulatory safeguards

SWAMI identified some serious legal problems when applying the existing legal framework to address the intricacies of an AmI environment. We found that most of the challenges arising in the new AmI environment should be addressed by transparency tools (such as data protection and security measures). Transparency should be the default position, although some prohibitions referring to political balances, ethical reasons or core legal concepts should be considered too[6].

A set of rules needs to be envisaged to guarantee procedural safeguards similar to those currently applicable to the protection of our homes against state intervention (e.g. requiring a search warrant). Technical solutions aimed at defending private digital territories (the private sphere of the individual no matter where he is) against intrusion should be encouraged and, if possible, legally enforced. The individual should be empowered with the means to freely decide what kind of information he or she is willing to disclose. Such protection could be extended to the digital movement of the person, that is, just as the privacy protection afforded the home has been or can be extended to the individual's car, so the protection could be extended to home networks, which might contact external networks.

All employees should always be clearly and a priori informed about the employee surveillance policy of the employer (when and where surveillance is taking place, what is the finality, what information is collected, how long it will be stored, what are the (procedural) rights of the employees when personal data are to be used as evidence, etc.).

The status of pseudonymity under the law needs further clarification. A pseudonym prevents disclosure of the real identity of a user, while still enabling him to be held responsible to the other party if necessary. It may provide a privacy tool, and remedy against profiling. Using different pseudonyms also prevents the merging of profiles from different domains. It is, however, unclear what is the legal status of pseudonyms (whether they should be regarded as anonymous data or as personal data falling under the data protection regime).

The obligation of data protection law to inform the data subject about when and which data are collected, by whom and for what purpose gives the data subject the possibility to react to mistakes (and thus to exercise his right to rectification of data) or abuses, and enables him to enforce his right in case of damage. It would be desirable to provide the individual not only with information about what data relating to him are processed, but also what knowledge has been derived from the data. This might imply a rethinking of data protection law.

A means to prevent data laundering could be envisaged which would create an obligation for those who buy or otherwise acquire databases, profiles and vast amounts of personal data, to check diligently the legal origin of the data. Without checking the origin and/or legality of the databases and profiles, one could consider the buyer equal to a receiver of stolen goods and thus held liable for illegal data processing. An obligation could be created to notify the national Data Protection Officers when personal data(bases) are acquired. Those involved or assisting in data laundering could be subject to criminal sanctions.

Profiling practices and the consequent personalization of the ambient intelligence environment lead to an accumulation of power in the hands of those who control the profiles and should therefore be made transparent.

Who should implement which safeguards

Simply identifying safeguards is not sufficient, of course, so the SWAMI consortium went further and specifically addressed recommendations to the European Commission, Member States, industry, academia, civil society organizations and individuals. Among our recommendations were the following:

Recommendations for the European Commission

The Commission should ensure that privacy, identity, trust, security and digital divide issues are taken into account in any project it supports.

Research on technologies that could help protect our privacy and strengthen the security of networks and devices (against attackers and other vulnerabilities), and that could help to minimize the digital divide should be increased.

Consultations like that undertaken by the EC on RFIDs[7] should be considered with regard to other relevant technologies and concepts, e.g. biometrics and interoperability. The implications for privacy caused by other technologies, such as location-tracking systems, physiological sensors, video and audio sensors should be evaluated, and good practices in use of these technologies should be developed and widely promulgated.

A legal framework for sharing knowledge from AmI-generated profiles should be developed, as well as legal protection of technical solutions enabling such information management. A legal framework is needed to cover automated protocols for privacy policy negotiations as well as automated schemes that imply the consent of the data subject. The legal framework should cover situations wherein the explicit consent of the data subject for each collection of data is replaced by a ''consent'' given by an intelligent software agent.

The Commission should consider development of legal rules with regard to issues that are specific to AmI. In that respect, we propose that legal schemes be developed for digital territories as an important safeguard of privacy in the digital world of AmI. Especially, we propose that such territories be protected against unlawful and unnecessary interference. The specific legal schemes would also be necessary to address the use of software agents and privacy-enhancing technologies (PETs).

The Commission should take steps to ensure that the consumer is always aware of any potentially privacy-threatening software or device embedded in any product he purchases. Product warnings and consumer notifications should always be in place.

Recommendations for the member states

In the procurement of ICT products or services, Member States should give emphasis to critical issues such as security and trustworthiness.

Member States should consider introducing legislative prohibitions on the admissibility (or general acceptance of the exclusionary rule) of evidence obtained through privacy and/or data protection law infringements.

Appropriate authorities (e.g. the Data Protection Officer) should control and authorize applications of implants after the assessment of the particular circumstances in each case. When an implant enables tracking of people, people should have the possibility to disconnect the implant at any time and they should have the possibility of being informed when a (distant) communication (e.g. through RFID) is taking place.

Governments that have not yet done so should ratify the Cybercrime Convention. The Convention should have a ''revision'' mechanism so that signatories could negotiate and include in the convention definitions of new, emerging cybercrimes. Specific provisions criminalizing identity theft and (some forms of) unsolicited communication could be included within the scope of the convention.

A means to prevent data laundering could be an obligation imposed on those who buy or otherwise acquire databases, profiles and vast amounts of personal data, to check diligently the legal origin of the data.

Following the subsidiarity principle, Member States and/or regional or local authorities should take responsibility for improving citizen awareness and education in regard to privacy, identity, security and trust issues associated with AmI.

Recommendations for industry

Industry should recognize that it is in their interest to reduce consumer distrust by enhancing transparency by effectively informing users about system procedures, purposes and responsibilities about latent operations and what measures they have put in place to avoid data misuse. Industry should take the initiative to ensure that any networked device, particularly those used by consumer-citizens, comes with a privacy warning much like the warnings on tobacco products.

All employers should clearly inform employees about their employee surveillance policy.

Organizations that compile databases with personal data (even if such compilation is incidental to their primary lines of business) should state on their websites and on their products to what extent they are compliant with ISO 17799 (ISO, 2005) and/or how they have implemented the standard. An organization could also mention to what extent they follow other guidelines dealing with privacy and security, such as those produced by the OECD[8].

Industry should expend less effort on fighting new regulations and more effort on involving stakeholders in the assessment and management of risks to privacy, identity, trust, security and inclusiveness. Involving stakeholders at an early stage will minimize downstream risks.

Recommendations for civil society organizations

An alternative to peer-rating systems are credibility-rating systems based on the assessment of trusted and independent institutions, such as library associations, consumer groups or other professional associations with widely acknowledged expertise within their respective domains. Ratings should be based on systematic assessments against clearly defined quality standards.

Consumer associations and other civil society organizations (CSOs) could play a useful role as a mediator between service providers and individual consumers and, more particularly, in forcing the development of service contracts (whether real or implicit) between the service provider and the individual consumer. Consumer organizations could leverage their negotiating position through the use of the media or other means of communication with their members. CSOs could position themselves closer to the industry vanguard as represented in platforms such as ARTEMIS[9] by becoming members of such platforms themselves. Within these platforms, CSOs could encourage industry to develop ''best practices'' in terms of provision of services to consumers.

Recommendations for academia

Institutes of higher education should ensure that courses in ICT-relevant disciplines address:

- impacts of ICT on society;
- knowledge from technology assessment or from ''impact and design research''; and
- promotion of awareness of development potential for health and the environment in the development phase of new technologies.

Universities should (continue to) participate in the development of technological safeguards, such as privacy and security protection in networks (including mobile, ad-hoc and sensor networks, as well as personal area networks), in personal devices and in smart spaces, in identity management systems and in developing technological means to minimize the digital divide (such as user interfaces for all, language translation tools and e-learning methods).

Recommendations for individuals

Users cannot be innocent bystanders and expect others to look after their interests with regard to privacy and security aspects of the emerging AmI world. We concur with the OECD when it says ''Participants [including individual users] should be aware of the need for security of information systems and networks and what they can do to enhance security . . . Participants should be aware of the . . . good practices that they can implement to enhance security, and the needs of other participants'' (OECD, 2002, p. 10). At the same time, we

recognize that such good advice will not (cannot) be taken onboard by all users, children and the elderly being the most obvious example.

Priority recommendations

SWAMI identified many threats and vulnerabilities and many safeguards for dealing with them – perhaps too many. Hence, SWAMI partners decided to prioritize our top recommendations and the following are our top seven:

1. The Commission, together with Member States, perhaps under the auspices of the European Network and Information Security Agency (ENISA)[10], should initiate a formalized risk assessment / risk management process with regard to the risks posed by AmI to security and privacy. We recommend that the assessment and decision-making process be open, transparent and inclusive, that stakeholder groups be identified, contacted and encouraged to take part in the process. Individuals should also be given an opportunity to express their views. Such a process could be initiated by means of a green paper on the risks to security and privacy in an AmI world. Whatever the outcome of the process, we recommend that the risk assessment be undertaken again (and again) in the future with some regularity, the periodicity of which might depend on the rapidity with which AmI is deployed (bearing in mind that the technologies for AmI are already being developed and deployed).

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, but especially the public that AmI is on its way, that it offers great benefits, but also poses certain security and privacy risks. There are many ways of raising awareness (through education, the media, etc), but to give this recommendation some specific focus, we recommend that Member States hold annual national contests which would offer some form of recognition to the best product or service offering privacy and security protection. We recommend a run-off at European level. This could be a counterpoint to the notoriously bad publicity that ambient intelligence (especially RFID applications) has received in recent years[11]. Any such campaign aimed at informing the public about ambient intelligence services and at inspiring trust should involve *all* stakeholders, and any such competition should be judged by independent evaluators.

3. The Commission and Member States should review carefully the third SWAMI report on threats, vulnerabilities and safeguards and address the inadequacies and lacunae in the existing legal and regulatory framework with respect to AmI. Law is only one of the available tools for regulating behaviour, in addition to social norms, market rules and the ''code'', i.e. the architecture of the technology (e.g. cyberspace, ambient intelligence, mobile telephony).

4. Member States should meet the challenges of AmI by legal instruments that do not prohibit new technological developments, but channel them (such as by data protection and security measures). Transparency should be the default position, although some prohibitions referring to the political balances, ethical reasons or core legal concepts should be also considered in policy discussion. 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 the changes of context, in which privacy and other legal issues are context-dependent.

5. The biggest weakness in enforcement of rights is the limitation of any European rule to Member States only, or to countries that have signed international conventions such as the Cybercrime Convention. Clearly, ICTs and AmI have global dimensions. International co-operation in developing and enforcing the legal framework is necessary. Therefore, the Commission and Member States should be proactive in the development of a more comprehensive international co-operation framework that takes AmI technologies and capabilities into account as a matter of urgency.

6. The European Commission should ensure that projects that it funds take societal impacts and, in particular, privacy, security and trust issues into account. Currently, EC calls say

that project participants must conform to relevant EU legislation, *inter alia*, the data protection directive (95/46/EC). It is, of course, necessary that project participants (or any third party funded by the EC) conform to EU legislation, but we think the Commission should be more demanding – i.e. it should require those it funds to specifically speculate what privacy or security impacts might arise from their projects and what measures should be taken to address those. In other words, simply conforming to legislation is not enough. Project participants must be asked to foresee or even to speculate what privacy or security implications their projects *might* have. By the same token, the EC proposal and tender evaluators should also be asked to evaluate project proposals and tenders from the same optic. We recommend that Member States adopt a similar approach.

7. We would like to especially emphasize the importance of the Commission, Member States and others funding research on technological safeguards for protecting privacy and enhancing security and for overcoming the digital divide. If technology does not provide solutions for human-technology interfaces for all, or for user-friendly security, other safeguards will not be able to solve the problem. We suggest that among technological safeguards research on intelligent algorithms is especially important.

Conclusion

In an ambient intelligence world, an increase in security (in the sense of measures to ensure the safety of society) most likely *will* encroach upon our privacy. Surveillance cameras *will* continue to proliferate. We can assume that, no matter what privacy protections government and business *say* they honor, our telecommunications, e-mails and Internet usage will be monitored to increasing degrees. The same will be true of our interfaces with the world of ambient intelligence. The products we buy and use will be linked to us. Personal data will be mined, linked and processed, traded, shared and sold. Many such practices will be unjustified and will violate our rights and civil liberties. We assume or should assume that those encroaching upon our rights and civil liberties will not only be criminals, but (supposedly) legitimate businesses and governments. Even so, the majority of the population may be willing to accept such encroachments because they are genuinely concerned about their own security (= safety), that of their family and fellow citizens. The so-called war on terror has undoubtedly provided fertile ground for acceptance[12].

We can assume that gains in security will be made at the expense of losses in privacy[13]. We do not see an easy solution to this problem: indeed, there may not be any. Perhaps the most we can hope for is that unjustified encroachments, abuses and violations will come to light and be redressed. Coupled with this unhappy prospect is the need for users to be aware, to be vigilant at all times when and where their privacy is put at risk or might be at risk and what users can do, individually and collectively, to minimize those risks. We trust that the safeguards we have suggested can go some distance towards minimizing those risks.

SWAMI partners believe that, sooner or later, we will live in a world of ambient intelligence. 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 cognizant of the threats and vulnerabilities and work together to ensure adequate safeguards exist. Certainly, industry should become more active in creating applications that are secure and privacy-enhancing since this is the best 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.

Notes

1. The SWAMI consortium comprises the Fraunhofer Institute for Systems and Innovation Research (Germany), Technical Research Center of Finland (VTT Electronics, Finland), Vrije Universiteit Brussel (VUB, Belgium), Trilateral Research & Consulting (UK) and the Institute of Prospective

Technological Studies (IPTS, Spain) of the European Commission's Joint Research Centre. The website is: http://swami.jrc.es

2. For a review of these, see Wright (2005).
3. Cf O'Harrow, Robert (2005, p. 107), ''We have created a unique identifier on everybody in the United States,'' said [Ole] Poulsen, the company's [Seisint Inc.] chief technology officer. ''Data that belongs together is already linked together.''
4. http://europa.eu.int/information_society/soccul/eincl/index_en.htm
5. The SWAMI reports can be downloaded from http://swami.jrc.es
6. On the differences between ''tranparency'' and ''opacity'' (resp. regulation and prohibition) see De Hert (2001, 2002), Serge (2006).
7. www.rfidconsultation.eu/
8. See notably OECD (2001, 2002).
9. ARTEMIS is the acronym for Advanced Research and Development on Embedded Intelligent Systems. It is one of about 30 European Technology Platforms (ETPs), a kind of public-private partnership which aims to mobilize and co-ordinate private and public resources to meet business, technical and structural challenges in embedded systems and to ensure that systems developed by different vendors can communicate and work with each other via industry standards.
10. www.enisa.eu.int/
11. RFID technologies and their promoters have received Big Brother Awards in various countries. See, e.g. http://bigbrotherawards.de/2003/.cop/; www.edri.org/edrigram/number4.3/frenchbba?PHPSESSID = a08c4d85ac916daab3d8660a1d377dd8; www.privacyinternational.org/article.shtml?cmd%5B347%5D = x-347-187899; www.bigbrotherawards.cz/en/winners_2005.html. See also Albrecht and McIntyre (2005).
12. ''Since the 2001 terror attacks, a slim majority of the American public has favored protecting security over preserving civil liberties, according to opinion pollsters'' (Mohammed *et al.*, 2006). This is not to say, of course, that everyone accepts such encroachments. See, for example, Hosein (2005, p. ii): ''Though the Open Society is in peril, there is much to be hopeful for. This report finds that in the US there is a continuing debate surrounding anti-terrorism policies'' See also the following end note.
13. Security expert Bruce Schneier has commented, ''We're not trading privacy for security; we're giving up privacy and getting no security in return'' (Schneier, 2005).

References

Albrecht, K. and McIntyre, L. (2005), *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, Nelson Current Publishers, Nashville, TN.

De Hert, P. and Gutwirth, S. (2006), ''Privacy, data protection and law enforcement: opacity of the individual and transparency of power'', in Claes, E., Duff, A. and Gutwirth, S. (Eds), *Privacy and the Criminal Law*, Intersentia, Antwerp/Oxford, pp. 61-104.

European Commission (EC) (2003), ''Work Programme for the specific programme for research, technological development and demonstration: 'Integrating and strengthening the European Research Area''', specific activity covering policy-orientated research under ''Policy support and anticipating scientific and technological needs'' (SSP Call 3), Brussels.

Hosein, G. (2005), *Threatening the Open Society: Comparing Anti-Terror Policies in the US and Europe*, Privacy International, London, available at: www.privacyinternational.org/issues/terrorism/rpt/comparativeterrorreportdec2005.pdf

Information Society Technologies Advisory Group (ISTAG) (2003), *Ambient Intelligence: From Vision to Reality*, Office for Official Publications of the European Communities, Luxembourg, available at: www.cordis.lu/ist/istag-reports.html

ISO (1999), *Information technology – Security techniques – Evaluation criteria for IT security (ISO/IEC 15408)*, 1st ed., International Organization for Standardization, Geneva.

ISO (2005), *Information Technology – Security techniques – Code of Practice for Information Security Management (ISO/IEC 17799)*, International Organization for Standardization, Geneva.

Mohammed, A. and Kehaulani Goo, S. (2006), ''Government increasingly turning to data mining'', *The Washington Post*, June 15, available at: www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html

OECD (2001), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Co-operation and Development, Paris.

OECD (2002), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Organisation for Economic Co-operation and Development, Paris.

O'Harrow, R. (2005), *No Place to Hide*, Simon & Schuster, New York, NY.

Schneier, B. (2005), ''Why data mining won't stop terror'', *Wired News*, March 9, available at: www.schneier.com/essay-108.html

Stajano, F. and Anderson, R. (2002), ''The resurrecting duckling: security issues for ubiquitous computing'', pp. 22-6, first Security & Privacy supplement to *IEEE Computer*, April, pp. 22-26.

Wright, D. (2005), ''The dark side of ambient intelligence'', *info*, Vol. 7 No. 6, pp. 33-51.

Corresponding author

David Wright can be contacted at: david.wright@ trilateralresearch.com