The dark side of ambient intelligence

David Wright

David Wright is a co-founder and managing partner of Trilateral Research & Consulting LLP, London, UK. He specialises in policy and regulatory issues relating to ambient intelligence, risk and impact assessment. E-mail: david.wright@trilateralresearch.com

Abstract

Purpose – *To survey ambient intelligence research in Europe, the USA and Japan and, in particular, in the context of the issues of privacy, identity, security and trust and the safeguards proposed to protect them.*

Design/methodology/approach – *This paper is based on research being conducted by the SWAMI consortium under the EC's Sixth Framework Programme. SWAMI stands for Safeguards in a World of Ambient Intelligence. The consortium comprises five partners: the Fraunhofer Institute (Germany), the Technical Research Center of Finland (VTT Electronics), Vrije Universiteit Brussel (Belgium), the Institute for Prospective Technological Studies (IPTS) (Spain) and Trilateral Research & Consulting (UK). The 18-month SWAMI project began in February 2005.*

Findings – *Most AmI projects do not take into account privacy, security and related issues. However, a reasonable number do (perhaps a quarter of those in Europe) to a greater or lesser extent and some have proposed safeguards.*

Research limitations/implications – *This paper references only a limited set of the research projects being carried out in Europe, the USA and Japan. More detailed information can be found on the SWAMI web site (http://swami.jrc.es).*

Practical implications – *A mix of different safeguards will be needed to adequately protect privacy, etc. in the new world of AmI.*

Originality/value – *Until now, there has been no reasonably comprehensive survey of AmI research projects in Europe, the USA and Canada focused on privacy, security, identity and trust issues. None has considered the range of safeguards needed to protect privacy, etc.*

Keywords *Intelligence, Computers, Privacy, Data security, Trust*

Paper type *Research paper*

Introduction

The brave new world of ambient intelligence is almost upon us. For those who have not been watching the future, ambient intelligence is the buzz phrase describing a world in which ''intelligence'' is embedded in virtually everything around us. It's been called an internet of things, where radio frequency identification (RFID) tags are attached to all products. It's a world of smart dust with networked sensors and actuators so small as to be virtually invisible, where the clothes you wear, the paint on your walls, the carpets on your floor, the paper money in your pocket have a computer communications capability. It's a 4G world where today's mobile phone is transformed into a terminal capable of receiving television, accessing the internet, downloading music, reading RFIDs, taking pictures, enabling interactive video telephony, and much more. It's a world of convergence, where heterogeneous devices are able to communicate seamlessly across today's disparate networks. It's a world of machine learning, where computers monitor our activities, routines and behaviours to predict what we will do or want next and, hey, presto!, there it is. In the brave new world of ambient intelligence, we'll never have to worry about losing track of granny or junior because they'll have a location device implanted under the skin or, if they're squeamish about that, then at least they'll have one in their wristwatch.

Different buzz words have been used to refer to this brave new world. In Europe, we use ambient intelligence (AmI), a term coined by Emile Aarts of Philips and adopted by the European Commission and just about everyone else in Europe. In America, its equivalent is ubiquitous or pervasive computing, and in Japan, they use ubiquitous networking. Some have referred to the disappearing computer or invisible computing, but essentially all these terms mean much the same thing: researchers in Europe, the USA and Japan are all exploring and developing similar technologies and dealing with similar problems.

This future world was first spotted in 1991 by Mark Weiser, chief scientist at the Xerox Palo Alto Research Center (PARC) in California. That's when he published a paper in *Scientific American* which spoke of a third generation of computing systems. He coined the term ubiquitous computing to describe an era when computers would vanish into the background.

Benefits

Ambient intelligence is expected to yield many benefits for citizens and consumers, industry, commerce and the provision of public services. Information Society Technologies Advisory Group (ISTAG), the committee which advises the EC's Information Society Directorate General, sees ''significant opportunities'' for AmI in relation to:

- Modernising the European social model, particularly in terms of: improving civil security; providing new leisure, learning and work opportunities within the networked home; facilitating community building and new social groupings; providing new forms of healthcare and social support; tackling environmental threats; supporting the democratic process and the delivery of public services.
- Improving Europe's economy in terms of: supporting new business processes; increasing the opportunities for tele-working in the networked home; enhancing mobility and improving all forms of transport; supporting new approaches to sustainable development (ISTAG, 2003, p. 9).

It has attracted a lot of interest in Europe, the USA, Japan and other countries, from their governments, industry, universities, research institutes and other stakeholders. Hundreds of millions of euros have been spent and are being spent on AmI projects.

Realisation of the AmI vision, however, poses many challenges, many of which are technical, some of which are what might be described as organisational, and still others which involve societal issues.

The dark side

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 the very nature of AmI, i.e. the fact that AmI technologies will deliver personalised services to users means that somewhere a lot of personal information needs to be stored about the user. That being the case, there are risks that the user's personal information can be abused, either accidentally or intentionally. These risks have been recognised by policy-makers and researchers. ISTAG said the anticipated benefits of ambient intelligence may be numerous but the enabling technologies can also facilitate monitoring, surveillance, data searches and mining, as a result of which AmI deployment is likely to be of great concern to citizens, civil liberties groups, governments and industry. Addressing the balance between privacy and security will, it says, be a core challenge for the future. It is also at the heart of the SWAMI project.

Enabling technologies

At the most basic level, AmI is enabled by three core technologies: cheap, low-power computers, a network that ties them all together and software systems implementing ubiquitous applications. However, there are many permutations of these technologies, including RFIDs and their readers, sensors, actuators, displays, power sources, including those that ''scavenge'' power, etc. As a result, one ends up with many heterogeneous components in diverse networks which somehow have to interconnect as part of vast new

architectures enabling context awareness, machine learning and personalisation of services on a hard-to-imagine scale.

In fact, the construction of the ambient intelligence space has already begun. Sensors and actuators, key AmI technologies, have been in use for decades as a result of the exponential increase in electronic capabilities. Cars on the road today have 80 or more embedded sensors and actuators. What is new is that such devices are being networked and their numbers are set to increase by orders of magnitude. Meanwhile, location aware services have prompted concerns, even though they also offer many benefits. The increasing use of GPS in mobile phones in the USA in conjunction with services such as uLocate and Wherify Wireless enables those with mobile phones to be tracked wherever they go. While helping parents to know where their children are, the risks of unwanted and unwarranted surveillance have been highlighted by privacy advocates and others. The dramatic reduction in the cost of computing and communications and the rise of the internet are laying the foundations for the scenarios envisaged for the future. Above all, the networking of the proliferating devices in recent years demonstrates that the future, despite the still remaining formidable technological challenges, is not so far off.

Some of these technologies have already begun to ring alarms. In November 2003, some 30 privacy advocacy groups joined together to produce a position paper calling for a halt to the deployment of RFIDs until certain public policy issues are resolved[1]. Tags on or near individuals can be read without their knowledge. The tags can potentially be on everything in an individual's possession. RFID systems enable at least a scaling up, if not a change in the nature of surveillance and in the character of information collection that is possible (Borriello *et al.*, 2004, p. 23).

Ambient intelligence in Europe

The principal AmI sponsor in Europe has been and continues to be the European Commission. Industry, universities and some member states have also devoted time and money to AmI research, but by far the biggest sponsor has been the Commission, notably under its Fifth and Sixth Framework Programmes (FP5, FP6). Of the 60 EC-sponsored projects which SWAMI partners have reviewed, the largest project in euro value has a budget of €24 million and the smallest had a budget of €200,000. The average value was €4.7 million.

Virtually all of the European AmI projects have been undertaken by consortia, with an average number of 11 partners per project. Consortia typically comprise partners from different countries and different sectors, especially universities and industry.

As these numbers indicate, hundreds of millions of euros are being spent on AmI and hundreds of European companies, universities and others are participating collaboratively in taking AmI from vision to reality.

Ubiquitous computing in the USA

There has been and continues to be a huge amount of research on ubiquitous computing in the USA. Much of the research on ubiquitous computing has been undertaken in the universities, such as the University of California at Berkeley, Stanford, Cornell, Carnegie Mellon, Yale and Harvard. They have been heavily supported by government funding. The largest pool of funding for research is that of the Defense Advanced Research Projects Agency (DARPA), which is the central research and development organisation for the Department of Defense (DoD).

Probably the next most important source of funding is the National Science Foundation (NSF), an independent federal agency with an annual budget of $5.5 billion, funding 20 per cent of all federally supported basic research in US colleges and universities. The Department of Homeland Security (DHS) is growing in importance as a source of funding for cyber security research.

Many large companies have been undertaking ubiquitous computing research, either on their own or in consortia with other companies and/or universities. Among the companies are

Microsoft, IBM, Xerox, HP, Intel, Motorola, Cisco Systems, Sun Microsystems, etc. We have not made a determination of the overall funding by the corporate sector of research on ubiquitous computing, but to give one indicative example, IBM has said it plans to spend $250 million during the next five years on embedded technology and has created a ''sensors and actuators'' unit to that end (Ricadela, 2005).

Ubiquitous networking in Japan

As in Europe and the USA, the development of a ubiquitous network society can be truly said to be a national strategy. Considerable effort and resources are being invested in realising the strategy from all sectors, governmental, industry and academic.

The Ministry of Internal Affairs and Communications (MIC) has been the most important sponsor and policy-setter, but other ministries such as the Ministry of Education, Culture, Sports, Science and Technology (MEXT) and the Ministry of Land, Infrastructure, and Transport, are also involved.

From industry, NTT DoCoMo, KDDI, Hitachi, NEC, Fujitsu, Nomura Research Institute, Matsushita, Mitsubishi, Toshiba and Toyota and many others feature in ubiquitous networking research, especially in the context of third and fourth generation mobile (3G, 4G).

Among the most important universities where ubiquitous networking research is undertaken are University of Tokyo, Tokyo University of Technology, Keio University, Kyushu Institute of Technology, Tokyo Denki University and Waseda University.

The National Institute of Information and Communications Technology (NICT), an incorporated administrative agency, and various associations such as Telecom Information Sharing and Analysis Centre (Telecom-ISAC) Japan have also been participants.

From visions to platforms

We have structured our review of research in Europe, the USA and Japan according to visions, scenarios, roadmaps, research agendas and projects, as each category is distinct and serves a different purpose, although one leads logically to the next[2]. As one might expect, not all of these visions, scenarios, roadmaps, research agendas and projects have taken the issues of privacy, identity, security and trust into account, although many have. We also consider the platforms, i.e. the way in which industry, governments and other stakeholders have organised themselves to undertake the shared research agendas. We then draw the reader's attention to the key issues of privacy, identity, security and trust, point out safeguards that have been proposed and draw certain conclusions.

Visions

Many projects have visions of what they want to do or, more expansively, of the future world of ambient intelligence, but most are not elaborated much beyond a simple vision statement, but in the AmI field, one can find whole reports dedicated to their visions of the future, though they are few in number. The most important are the following:

Europe

Perhaps the best-known vision document is *The Book of Visions* (Wireless World Research Forum (WWRF), 2001), which provides a vision of our technological future, or at least our wireless technological future. It resulted from an initiative of several large European companies and Motorola who came together to form the WWRF. The first version of the *Book* appeared in 2001[3]. The vision was of a future 10-15 years away and it included ambient intelligence within its scope.

An equally well-known AmI vision was produced by ISTAG, which, in September 2003, published a report called *Ambient Intelligence: From Vision to Reality*. Its report should be read in conjunction with at least two other ISTAG papers. One is on scenarios (see below), the other is on security and privacy issues (ISTAG, 2002).

The USA

There may seem to be fewer vision reports on ubiquitous computing in the USA, but this does not mean, of course, that there are not visions of the brave new world. On the contrary. It's been said that the *Embedded Everywhere* report published by the National Academy of Sciences (NAS) is such a vision document, but in fact it is explicitly a research agenda. Nevertheless, as its title suggests, it does contain some visions of the future. With networking sensors embedded everywhere, it foresees the day when we will have an internet of things.

Japan

Japan's vision of and strategy for a ubiquitous network society has been shaped by, especially, three documents (or rather sets of documents). The first are the NRI Papers produced by the Nomura Research Institute, several of which were authored by Teruyasu Murakami[4]. Evidence would suggest they have been very influential. The Ministry of Internal Affairs and Communications (MIC) chose him to chair the policy roundtable which generated the December 2004 report on which Japan's current ubiquitous network society strategy is based. In addition to the NRI Papers and the MIC's own reports, the Mobile IT Forum (mITF) produced a vision document, which is also a roadmap and a platform, all rolled into one, called the *Flying Carpet* (mITF, 2004).

More details of the government's strategy to achieve the u-Japan vision can be found in an MIC White Paper, published in 2004, with the somewhat grandiose title ''Building a ubiquitous network society that spreads throughout the world''[5].

Scenarios

From visions, one can build scenarios. Building scenarios is a useful tool for the development and application of new technology. Scenarios could be seen as akin to storytelling, as a way of projecting new situations showing the application and/or consequences of new technologies. Scenarios anchor the design process and, at the same time, are intended to provoke reflection on situations of use, both as they occur in the real world and in the future.

There are different types of scenarios. Most scenarios show the benefits of AmI or deal with specific issues, but there are a few ''dark'' scenarios including those constructed by the SWAMI project. Often what makes a scenario ''dark'' are deficiencies with regard to privacy, security, identity and other socio-economic issues.

Below are a few examples.

Undoubtedly the best-known ambient intelligence scenarios in Europe are those produced for ISTAG (Ducatel *et al.*, 2001). The ISTAG scenarios were actually developed by IPTS in collaboration with DG Information Society and 35 experts from across Europe. The aim was to describe what living with ambient intelligence might be like for ordinary people in 2010. The four scenarios centre on Maria, dubbed a ''road warrior'', Dimitrios and his ''digital me'' (D-Me) device, Carmen (a scenario about traffic, sustainability and commerce), and Annette and Solomon (a scenario about social learning in the ambient intelligence space).

The Information Technology for European Advancement (ITEA) has many scenarios within its 262-page roadmap (ITEA, 2004)[4] but the two most developed are about the Rousseau family's use of AmI as they go on holiday, and about a professional couple, Oliver and Vera, co-ordinating their separate itineraries from different cities in Europe so that they can meet while on their respective travels.

In the USA, the *Who Goes There?* report (Kent and Millett, 2003) has two very good scenarios to illustrate the ways in which identification and authentication arise in everyday life and to highlight some of the important issues associated with new systems. The first scenario concerns ''Joseph K'' as he goes on a business trip. The second describes a token-based authentication system used by Laura on a visit to a hospital.

From research done to date, few scenarios appear in papers about Japan's ubiquitous networking projects, at least, not developed to the extent that one finds in (especially) European and American projects. However, that does not mean scenarios are absent. The

Smart Hot-Spot project (see below) has a couple of relatively simple scenarios, which show use of smart furniture in daily life, one in the home and one at a train station (Ito *et al.*, 2003).

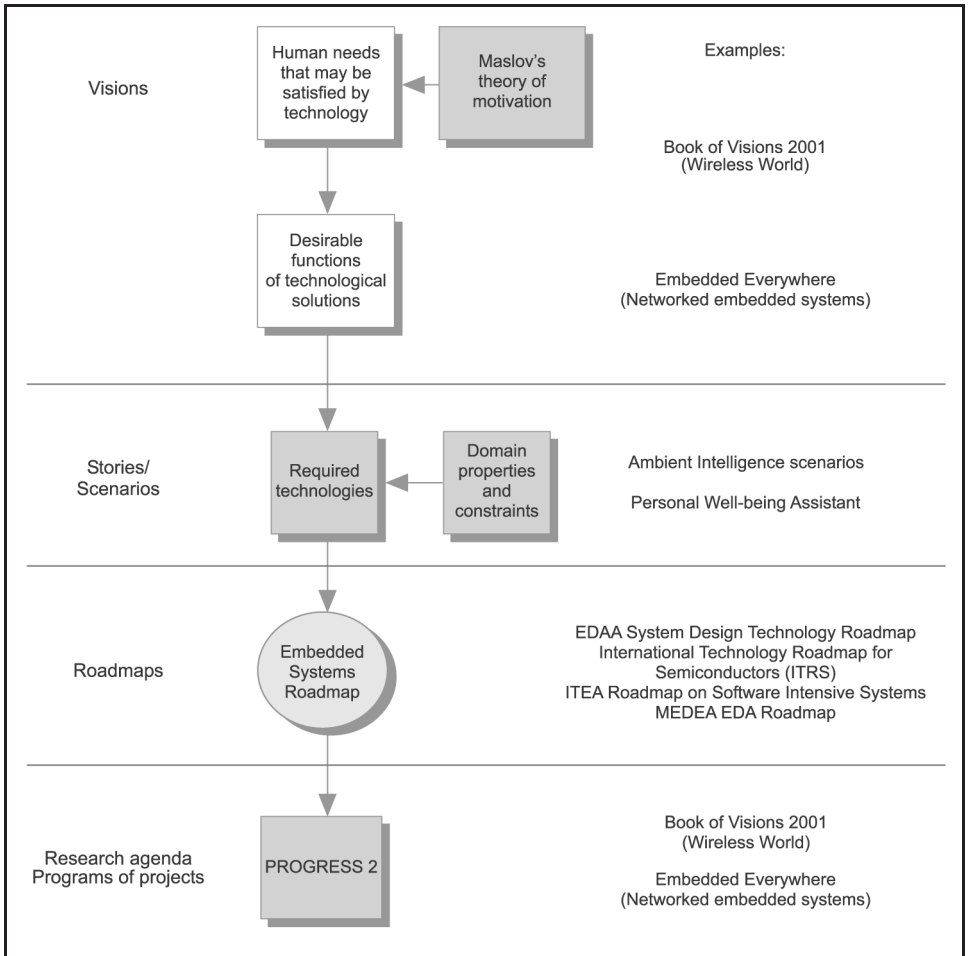
Not all scenarios need to be written, of course. The Ministry of Internal Affairs and Communications prepared a briefing package for the overseas press which has several ''images'' of the ubiquitous network society. On KDDI's web site, one can find several ubiquitous network scenarios in video format.

Roadmaps

Roadmaps follow on from scenarios, i.e. to realise a scenario, roadmaps set out what steps must be taken. Roadmaps have become a strategic planning tool in many industries and even in international diplomacy (e.g. the US-brokered Middle East roadmap). Roadmaps provide an overview of technology development by mapping out gaps, barriers and bottlenecks to be overcome.

There are several European AmI-relevant roadmaps, more than cited here. One of the first was the *Embedded Systems Roadmap* (see Figure 1) produced at the behest of the Technology Foundation STW, the Dutch funding agency for university research. Published in 2002, the roadmap focused on embedded systems design, including general trends, user needs, technology requirements, system validation, etc.

Figure 1 Positioning of the *Embedded Systems Roadmap*



Note: Reproduced with permission

The PAMPAS roadmap (June 2002-May 2003)[6] focused on ensuring that future mobile services and systems satisfy security, privacy and identity management requirements.

The RAPID project (July 2002-June 2003)[7] developed a strategic roadmap for applied research in the area of privacy and identity management.

The AMSD project (June 2002-August 2003)[8] was a dependability roadmap for the Information Society in general and embedded systems in particular. It investigated aspects of dependability, including reliability, safety, security, survivability and privacy.

Fewer instances of roadmapping in the USA have become evident from our research. One very well known roadmap, at least in the world of semiconductors, is the International Technology Roadmap for Semiconductors (ITRS), which is an assessment of the technological challenges and needs facing the semiconductor industry 15 years into the future and potential solutions. The ITRS roadmap is, however, a technical document and does not deal with the ''softer'' issues of privacy, identity, security or even applications of semiconductors.

The comment about the relative scarcity of scenarios in Japan also applies to roadmaps. Where in Europe the use of roadmaps is relatively common, they are almost absent (or at least not very visible in documents translated into English) in Japan. One notable exception is the roadmap in the *Flying Carpet* report. In order to steadily implement the u-Japan policy, the MIC has also developed a roadmap which identifies 31 items with a specific schedule to realise its objectives by 2010.

Research agendas

From roadmaps, research agendas can be developed which indicate what areas must be researched in order to bring visions into reality.

Quite a few European projects have developed research agendas important to AmI. Below are a few examples.

The AMSD roadmap developed a research agenda for dependability in embedded systems.

The OZONE project (November 2001-August 2004)[9] conducted a technology gap investigation, resulting in recommendations for research in the domain of efficient pervasive computing.

The eMobility platform (see the section on platforms below) has also published a strategic research agenda. The latest version is dated March 2005. A further revision is planned for September 2005. Major sections of its research agenda deal with ambient services, security and trust.

In the USA, the National Academy of Sciences (NAS) has published several important reports which have served as research agendas for embedded systems and ubiquitous computing. Among them are the *Embedded Everywhere* report (Estrin *et al.*, 1991), which is undoubtedly the best known, *Who Goes There? Authentication through the Lens of Privacy* (Kent and Millett, 2003), *Trust in Cyberspace* (Schneider, 1999), and, most recently, a summary report from a workshop on *Radio Frequency Identification Technologies* (Borriello *et al.*, 2004). Also, work has been proceeding on another report, *Privacy in the Information Age*, to be published towards the end of 2005.

Although the *Embedded Everywhere* report was published in 2001, it has lost none of its validity and continues to reward those who go through it. The report discusses five features that must, it says, be addressed from the outset in the design of networked systems of embedded computers (abbreviated to EmNets, a term used throughout the report): reliability, safety, security, privacy and usability, which are encapsulated in the term ''trustworthiness''.

EmNets, says the report, are capable of collecting, processing, and aggregating huge amounts of data. With the advent of large numbers of EmNets, the technological stage is set for unprecedented levels of real-time human monitoring. The sensors are cheap and

unobtrusive, the computing and communications costs are very low, and there will be organisations with the resources and motivation to deploy these systems. The temptation to use such systems for law enforcement, productivity monitoring, consumer profiling or in the name of safeguarding children from harm will be enormous. Consequently, says the report, privacy may be at much greater risk than at any previous time in history.

The *Flying Carpet* report is not only a vision document, it's also a research agenda. So, to a lesser extent, is the MIC's White Paper. Apart from those two documents, and the company-specific research agendas of corporate Japan, one could say that, to some extent, research agendas are being set by the various research laboratories, especially in universities, working on ubiquitous network society solutions. There are many such research laboratories, of which the following are perhaps the best known:

- the Aoyama-Morikawa Laboratory (AML) at the University of Tokyo;
- the Hide Tokuda Laboratory at Keio University;
- the Ubiquitous Computing Laboratory (UbiLab);
- the YRP Ubiquitous Networking Laboratory (YRP UNL);
- the Ubiquitous Networking Laboratory (UNL) at Tokyo Denki University;
- the Distributed and Ubiquitous Computing Laboratory at Waseda University.

Projects

There are many AmI projects in Europe, the USA and Japan, so those mentioned below are simply a few examples. Details of a much larger selection of projects can be found on the SWAMI web site.

Of the more than 70 European projects reviewed by SWAMI, about a fifth are devoted to privacy, identity and (personal) security issues or treat the issues in a substantive way. The four biggest projects (PISA, PRIME, FIDIS and GUIDE) had or have substantial budgets, ranging from €3.2 million and nine partners (PISA) to €13.14 million and 21 partners (PRIME). The privacy projects mainly focused on privacy enhancing technologies and identity management in the context of legal requirements. The PAMPAS and RAPID roadmaps were an exception; they dealt with non-technical aspects (socio-cultural, economic, legal). PISA and PRIME also dealt with legal requirements.

There are many projects in the USA dedicated to embedded technology. Most are undertaken by universities and industry, often with support from federal funding agencies such as DARPA, NSF, NASA, etc.

Smart Dust was a project at the University of California at Berkeley supported by the DARPA, among others. The project started in 1997 and finished in 2001, but many additional projects have grown out of it. The project developed tiny sensors, dubbed ''smart dust'', or motes, with wireless connectivity capable of organising themselves into flexible networks. The aim was to develop a complete sensor network node, including power supply, processor, sensor and communications, in a single cubic millimetre.

Similar in concept is Smart Matter, a project at the Palo Alto Research Center (PARC), a subsidiary of Xerox Corporation. The project began in the late 1990s, underpinned by micro-electro-mechanical systems (MEMS) which make it possible to mass produce large numbers of integrated sensors, actuators, computers and communication systems that can be embedded within products or spread throughout the environment.

Oxygen is a big, well-funded ($50 million) project (2000-2005) sponsored by industry and DARPA. Oxygen is an integrated software system that enables pervasive, human-centred computing through a combination of specific user and system technologies developed for use in the home, at work or on the move. The Oxygen goal was to make computation and communication as natural to use as the air we breathe.

With funding from DARPA, the Portolano project, at the University of Washington, is tagged as ''An expedition into invisible computing''. Invisible computing is a term coined by Donald

Norman to describe the coming age of ubiquitous task-specific computing devices. The devices are so highly optimised to particular tasks that they blend into the world and require little technical knowledge on the part of their users.

There are quite a few ubiquitous network projects in Japan. Little information is available on the sources and amounts of funding. Many of the projects have been undertaken by the laboratories mentioned above. There seems to be no projects on the scale of the largest European and American projects and none with large consortia of partners, as one finds in America and especially Europe. None of the projects has been specifically dedicated to privacy, security, identity and trust, although these issues figure in many of the projects to a greater or lesser extent. Examples of the Japanese projects are:

The Ubila project, sponsored by the MIC in co-operation with industry and academia, aims to realise ubiquitous networking, where computers and networks are present in all aspects of daily life.

Project STONE was initiated at the University of Tokyo in 1999 (and is continuing) to develop an innovative network architecture for supporting future ubiquitous computing applications.

The official name of the Yaoyorozu project (August 2002-March 2005) is ''Research on ubiquitous information society based on trans-disciplinary science''. The project has several partners and has received support from the Ministry of Education, Culture, Sports, Science and Technology (MEXT). Its principal research goal is desirable institutional systems and core technology for the ubiquitous information society in 2010.

The Micro Hot Spots project at Keio University employed ''smart furniture'', which can be used to convert non-smart space into a ''smart hot-spot''.

Platforms

There are many players in AmI development. To harness their efforts and ensure congruence, some organisational arrangements must be put in place. That is essentially the function of a platform. Technology platforms bring together companies, research institutions, financial institutions and regulatory authorities to define a common research agenda and to mobilise the necessary resources for implementing that agenda. Examples follow.

The WWRF includes manufacturers, network operators and service providers, R&D centres, universities, and small and medium enterprises (SMEs) among its open membership. As mentioned above, the WWRF produced *The Book of Visions*. One of the WWRF special interest groups (SIG2) deals with security and trust issues.

ARTEMIS is a sort of public-private partnership which aims to mobilise and co-ordinate private and public resources to meet business, technical and structural challenges in embedded systems. The organisational structure, extent of industry involvement, support from the Commission, all indicate that ARTEMIS is likely to be *the* European body with an overarching view and remit dealing with embedded systems.

eMobility is a mobile and wireless communications technology platform, established by European industry and operators in 2004, which, as noted above, is engaged in ambient intelligence service development.

In Europe, platforms are rather specifically defined and there are some good examples but there are rather few good examples in the USA. The apparent scarcity of platforms concerned the authors of the *Embedded Everywhere* report. They said that leaving EmNet work solely to the private sector raises a number of troubling possibilities. One great concern is that individual commercial incentives will fail to bring about work on problems that have a larger scope and that are subject to externalities: inter-operability, safety, upgradability, and so on. Moreover, a lack of government funding will slow down the sharing of the research, since commercial concerns tend to keep research private to retain their competitive advantage (Estrin *et al.*, 1991, p. 9). The authors added that EmNets will require changes in the way the nation's research enterprise is organised and that mechanisms need to be put in place for ensuring collaboration.

The director of the TRUST project made a similar point in his testimony before Congress. He said that a fundamental organisational problem is the lack of mechanisms for filling in the gap between the end of a successful federal research programme and the investment by the venture community and industry in products[10].

If we stretch the definition of platforms to include alliances, associations and lobby groups focused on ubiquitous computing and/or privacy and related issues, the following are noteworthy: the ZigBee Alliance; the Liberty Alliance; TRUSTe and the Electronic Privacy Information Center (EPIC).

From the research done so far, we have discovered few or no analogues in Japan to the platforms one finds in Europe. The platforms, such as they are, tend to be composed of industry full stop. This is not to say that the various stakeholders do not collaborate. They do, but in a different way. The Ministry of Internal Affairs and Communications, for example, will often initiate study groups, committees, councils and so forth, primarily composed of industry representatives, to provide advice and recommendations to the Ministry. Among the ''platforms'' working on the ubiquitous future are the Ubiquitous Networking Forum, the mITF, the TRON Association, the T-Engine Forum, the Ubiquitous Service Platform and the Trusted Mobile Platform.

Privacy

Information technology is increasingly all around us. Often we are not aware of its presence even now, let alone in a few years when the internet of things truly arrives. Alarmingly, at least for some, many people don't seem that bothered. They are quite willing, especially post 11 September, to forego some of their right to privacy in exchange for better security. However, some of the same profiling and data mining technologies used to improve security can also be used for surveillance and to bombard people with unwanted advertising.

There is some interesting discussion in *The Book of Visions* about profiling users, especially in the context of personalisation of services, security and privacy. It observes that without access to user-related context data many mobile services would not exist, nevertheless it recognises that customers should have the means to decide their security policies in a simple way. At the same time, this industry forum is of the view that ''profile data-exchange and accessibility must not be restricted too much'' in order to enable attractive and personalised mobile services (tailored to the user).

The *Flying Carpet* report says that according to its survey, privacy protection ranked higher among users than other 4G features. The MIC's White Paper offers similar findings from its survey. On the other hand, the latter survey found that only a small percentage of individuals take any measures to protect personal information.

Corporate Japan is well aware of the need to be sensitive to the privacy concerns of society. That concern was driven home in April 2005 when NTT DoCoMo issued a public apology for leakage of personal data of mobile phone subscribers[11]. DoCoMo said it took ''this incident very seriously and is implementing stringent measures based on Ministry of Internal Affairs and Communications guidelines on the protection of personal data to ensure that such a leak does not occur again.'' DoCoMo also said would penalise its president and CEO, a senior executive vice president and an employee who was in charge of the issue. (It didn't say what the penalties were.)

An even bigger theft of personal data was revealed in the USA in June 2005, when CardSystems Solutions, the payment processor for MasterCard, VISA and other credit card agencies, reported that 40 million credit card accounts may have been exposed to possible theft (Dash and Zeller, 2005).

With an internet of things, we can expect orders of magnitude more personal data to be collected than is the case today, which is already a lot. Among the biggest data aggregating companies in the USA are Acxiom, ChoicePoint, LexisNexis, Seisint, Verint, etc. How secure is the data they hold? Not very. They too have had data pilfered by hackers and non-hackers alike. As if theft wasn't bad enough, they have also put their vast databanks at the disposal of the CIA, FBI and other law enforcement authorities for surveillance purposes.

ISTAG posed a challenge for researchers, which can be paraphrased as follows: how can we ensure that personal data can be shared to the extent the individual wishes and no more? It's not an easy question to answer. Some safeguards can be adopted, but the snag is that profiling and personalisation, as indicated above, is inherent in AmI and operators and service providers invariably and inevitably will want to ''personalise'' their offerings as much as possible, and as they do, the risks to personal information will grow. Safeguards may help contain the risk but will never eliminate it. There are many unresolved issues. For example, in AmI networks, there are likely to be many operators and service providers, some of whom may be visible, some of whom will not be. Will consumers need or even be able to negotiate their level of protection with each one? If you want a particular service, will you have no choice except to forego some of your privacy? Are the privacy policies of operators and service providers satisfactory from the consumer's point of view? Can they be trusted? Are the data protection safeguards put in place by the operator or service provider adequate? If new AmI networks have a profile-learning capability, will the ''negotiated'' privacy protection rules still be relevant after a year or two of service?

Clearly, safeguards must be put in place. Government policy-makers require them, especially in Europe and Japan, but even in the USA, though to a lesser extent. The corporate sector is sufficiently intimidated by bad press and public pressure that they recognise that they must do something. Safeguards are discussed in greater detail below.

Identity

The US Federal Trade Commission estimates that more than 10 million Americans are victims of identity theft every year, which imposes a cost of about $5 billion on individuals and $48 billion on businesses. FTC statistics on identity and credit card theft indicate that only about 5 per cent of cyber criminals are ever caught.

Identity theft seems to be a bigger problem in the USA than in Europe and Japan, but it vexes policy-makers and the corporate sector there too. A number of initiatives and projects are underway to deal with the problem.

One recent initiative is that of the Liberty Alliance, which announced in June 2005 formation of a new multi-organisational group to combat identity theft. The Identity Theft Prevention Group is to serve as a hub for the global effort against identity theft. Liberty says the only truly effective solution is a balanced approach of technology and strong policy practices, as well as an educated public.

The concept of identity can be approached from a number of standpoints. We can view it from philosophical, psychological, sociological, legal and technical perspectives, which suggest there is a risk that identity management systems could be over-bearing in their complexity. The long term consequences of fixing identities may not be foreseen. Fixing identities may lead to function creep if an identity established for one purpose in one domain is reused in other domains for other purposes, as happens when a driver's licence is used to establish identity at a bank or shop.

ISTAG posed the challenge: How should we manage the relationship between identification and anonymity, so that authentication can be achieved without compromising privacy? Proving an identity is a matter of authentication, which in itself has its complexities. The *Who Goes There?* report's concluding chapter provides a toolkit that can aid in designing an authentication system sensitive to privacy concerns. It focuses on the three types of authentication:

1. *Individual authentication* is the process of establishing an understood level of confidence that an identifier refers to a specific individual.
2. *Identity authentication* is the process of establishing an understood level of confidence that an identifier refers to an identity. The authenticated identity may or may not be linkable to an individual.
3. *Attribute authentication* is the process of establishing an understood level of confidence that an attribute applies to a specific individual.

As the Information Society develops, the increasingly digital representation of personal characteristics changes the ways of identifying individuals. So-called virtual identities, perhaps embodying concepts such as pseudonymity and anonymity, are being created for security, profit, convenience, fun – and exploitation by others.

Trust

The lack of consumer trust is often cited as the reason why e-commerce (and e-health and e-government) via the internet is far from realising its potential. Attacks are not only becoming more numerous, they are becoming much more sophisticated. The software security firm Symantec observed that, in July 2001, ''Code Red spread to 250,000 systems within six hours and the worldwide economic impact of the worm was estimated at $2.62 billion. In the future, we may see the emergence of threats that infect vulnerable servers *in a matter of minutes or even seconds*''[12] (italics added). Such reports and pronouncements undermine trust and confidence.

ISTAG posed the challenge: what measures are there, and what standards should there be for dependability, trustworthiness, privacy? Quite a few projects in Europe, the USA and Japan address trust issues. One is called, appropriately enough, TRUST, the acronym for Team for Research in Ubiquitous Secure Technology, a project led by the University of California at Berkeley, with partners from nine universities and 11 big companies. With a $19 million contribution from the NSF[13], TRUST has proposed new software technology that would allow computers to determine whether a program is trustworthy. In addition to protecting computers against attacks, TRUST will consider ways to ensure that stored data remain intact and computer networks keep systems running properly even when intrusions occur – a concept known as ''degrading gracefully under attack''. Privacy, legal, societal and usability issues will be factored into the technology.

So far, in Japan as in the USA and Europe, the notion of trust in the ubiquitous network society has mainly focused on making networks trustworthy or, perhaps more precisely, of being able to use untrusted networks in a trustworthy way. Undoubtedly, this is all good stuff, but so far, there appears to be little research on the nature of trust, how trust can be earned, how it can be restored once it's been lost, user perceptions of what constitutes trustworthiness and the perceptions of different social groups. These sorts of aspects are important too, especially in view of intentions as articulated in the u-Japan policy to realise a society in which 80 per cent of Japanese accept ICTs as safe and friendly.

Security

A review of ubiquitous computing research in the USA needs to be seen against the backdrop of security, especially since 11 September 2001. Security was already an issue before then, but has been greatly magnified since. Security can be considered in the context of computer communications networks and systems and the infrastructures they support as well as in the context or from the perspective of individuals.

The importance of security as a subject of research in ubiquitous computing can be neatly summarised from a statement made by a computer scientist from the University of California at Berkeley before a Congressional committee. He spoke partly in support of the TRUST proposal which he and his colleagues had put together, but his remarks had wider relevance:

> Computer trustworthiness continues to increase in importance as a pressing scientific, economic, and social problem. The last decade has seen a rapid increase in computer security attacks at all levels, as more individuals connect to common networks and as motivations and means to conduct sophisticated attacks increase ... Cyber attacks are increasingly motivated by the financial gain and global politics. A parallel and accelerating trend of the last decade has been the rapidly growing integration role of computing and communication in critical infrastructure systems, such as financial, energy distribution, telecommunication and transportation, which now have complex interdependencies rooted in information technologies[10].

The US government drive to increase support for fundamental research in cyber security was abetted by a March 2005 report from the President's Information Technology Advisory Committee (PITAC) which said that the ''information infrastructure of the US is highly vulnerable to disruptive domestic and international attacks''. One big cyber security project into which the US government has put money is at the University of California-Berkeley. Called DETER (cyber Defense Technology Experimental Research network), the project provides a testbed for network defence and has partners from industry and other universities.

Japan's Ministry of Internal Affairs has set up a Study Group on Platform Functions for the Ubiquitous Network Society, which, among things, is developing measures necessary for ensuring security and safety. The group was expected to issue a report on its work in June 2005.

ISTAG has said that AmI will require security solutions very different from those of today's systems. It postulates a new security paradigm characterised by ''conformable'' security in which the degree and nature of security associated with any particular type of action will change over time and circumstance. ISTAG and others have said that any security rules must be user-friendly, intuitive and socially acceptable. eMobility says future service platforms must address new security requirements, among which it identifies:

- trusted platforms for mobile security and privacy;
- mobile application security and privacy;
- privacy-preserving mobile applications with tuneable anonymity;
- location-based services versus location privacy;
- secure transactions (especially mobile payments);
- secure content handling (DRM);
- secure interoperability between services offered to different environments (multi-technology and multi-operator covering both wireless and fixed access);
- user-centric mechanism allowing (authorising) controlled release of personal information;
- secure user identity management;
- single sign-on based on mobile authentication;
- authorisation privacy;
- authentication via security tokens using mobile devices; and
- defence and response to security attacks (Tafazolli *et al.*, 2005, p. 36).

Undoubtedly, security researchers are assured of continuing employment.

Safeguards

AmI projects in Europe, the USA and Japan have mooted various safeguards for protecting privacy and identity, enhancing security and trust. Among them are those described in the following sub-sections (see also Figure 2).

Privacy enhancing technologies (PETs)

An example of a PET is the Personal Well-being Assistant envisaged by the *Embedded Systems Roadmap*. The individual user would be able to control or set the features he or she wants, including his or her personal privacy settings, which could vary depending on the context or time or type of transactions to be performed. Even better, the PWA would be able to advise users if they weren't sure what level of privacy protection would be appropriate in a particular context.

Other potentially privacy enhancing technologies include biometrics but they also raise concerns about the security of the stored data against which biometric matches are made.

Figure 2 The μ-chip (mu-chip), Hitachi's response to resolving some of the issues associated with conventional RFID technology

Note: The μ-chip uses the frequency of 2.45GHz. It has a 128-bit ROM for storing the ID with no write-read and no anti-collision capabilities. Its unique ID numbers can be used to individually identify trillions of trillions of objects with no duplication. Moreover with a size of 0.4mm square, the μ-chip is small enough to be attached to a variety of minute objects including embedding in paper

Source: Courtesy of Hitachi

Also, biometrics may not be feasible in some instances, for example, due to some physical disability (blindness, absence of a hand, etc.). Like many other technologies, biometrics could be subject to abuse and may work to the detriment of privacy and identity protection.

Encryption has been a way of protecting communications and storage of personal data for many years, and inevitably will continue to be an important means of safeguarding privacy and identity and increasing security and trust in the AmI world as well.

An intelligent software agent (ISA) is software and/or hardware acting in order to accomplish a task on behalf of but with minimal intervention by the user. A software agent could run on a user's computer but could also move around on the internet or other networks. While executing its task, an agent can collect, process, store and distribute data. Some of these data could be about individuals and might be privacy-sensitive or become privacy-sensitive when the agent processes personal data or combines them with other data. The PISA project developed an ISA model to protect users' privacy in a networked environment.

Identity management protocols

Identity management protocols offer a good safeguard, if they do what they are intended to do. The Liberty alliance has developed specifications for federated identity and web services built on an open protocol called Security Assertion Markup Language (SAML), which it describes as device and platform ''agnostic''. Liberty collaborates with other standards bodies such as the Organization for the Advancement of Structured Information Standards (OASIS), which approved SAML 2.0 as a formal draft in March 2005. Liberty plans to start testing tools that incorporate SAML 2.0 in the summer of 2005. IBM has also been

developing cross-domain web identity authentication protocols. IBM says its browser-based attribute-exchange (BBAE) protocol is more privacy-friendly, scales better to multiple enterprise federations without any single point of control and provides authenticity and secure channel establishment in a realistic trust scenario.

Procedural safeguards

Taking note of a comment by Bruce Schneier (''Security is not about technology. It's about risks, and different ways to manage those risks'') (Schneier, 2003, p. 146), procedural safeguards should be on the list of safeguards. Procedural safeguards include actions such as privacy audits as well as physical security. Procedural safeguards could also include ''decommissioning'' RFID tags at the retail counter so that they are no longer functional when customers leave a store. But there are lots of holes in procedural safeguards. For example, the consumer might not be aware that RFIDs are being used in tagging certain products. Or the store might ''forget'' (accidentally on purpose) to decommission the tag.

Privacy policy standards

Currently, there are a wide range of privacy policies on corporate Web sites. Some aren't worth the cyber ink they've been written with. Often they are too long, written in legalese and don't provide any options to the prospective customer. The Platform for Privacy Preferences Project (P3P) has made some progress towards a simple, automated way for users to gain more control over the use of personal information on web sites they visit. P3P allows companies to make privacy promises, but additional tools are needed to help enforce these promises. While P3P was written for today's web, it can be considered as a useful starting point for the emerging Internet of things.

Legal and regulatory safeguards

The USA has not adopted legislation comparable to the data protection directive (95/46/EC) or the privacy and electronic communications directive (2002/58/EC) in Europe to build in safeguards for the protection of personal information. Indeed, the USA PATRIOT Act and other such legislation work at cross-purposes to the protection of privacy and increase the scope for surveillance of the citizenry. Some state governments, however, are passing new legislation (e.g. California law SB1386, effective July 2003) that forces organisations to inform individuals whenever there has been a privacy breach, and makes organisations liable for improper use of information.

Since there are no actual borders to information and communications networks, it is possible that an attack on networks will go beyond one country to cause increasing damage. The Council of Europe adopted the ''Convention on Cybercrime'' in November 2001 as a way of dealing with cross border cyber crime. So far, 37 countries, including Japan, have signed the convention but only five have ratified it.

In Japan, there are several pieces of legislation dealing with privacy protection, identity theft and security, including the so-called the Law Concerning the Liability of Internet Service Providers and the Unauthorised Computer Access Law. To deal with the problem of spam, Japan has adopted a ''Law on Regulation of Transmission of Specified Electronic Mail''.

The Japanese law concerning the protection of personal information (Law No. 57, 2003), which came into effect in April 2005, stipulates five basic principles regarding the collection and use of personal information: Information must not be used other than for clear, specified purposes; information must be collected properly; information must be always correct and up-to-date; information must be kept secure and safe from leakage; and information must be handled in a transparent manner that properly involves individuals.

Licensing

One novel approach to control the authorised dissemination of data about a user being considered by the Dutch PAW project are licensing techniques similar to those used in digital rights management. As many ambient systems are characterised by their low

resources and capabilities, PAW's key challenge is to develop an efficient architecture to implement its ideas.

Guidelines

US researchers have proposed several sets of guidelines aimed at protecting privacy and avoiding identity theft. Such guidelines are helpful as safeguards, but, of course, they are by themselves insufficient to ensure privacy truly is protected. Guidelines will not stop someone intent on violating privacy.

One set of guidelines can be found in the *Who Goes There?* report (Kent and Millett, 2003, p. 78). It recommends that, when designing an authentication system or selecting an authentication system for use, one should:

- authenticate only for necessary, well-defined purposes;
- minimise the scope of the data collected;
- minimise the retention interval for data collected;
- articulate what entities will have access to the collected data;
- articulate what kinds of access to and use of the data will be allowed;
- minimise the intrusiveness of the process;
- overtly involve the individual to be authenticated in the process;
- minimise the intimacy of the data collected;
- ensure that the use of the system is audited and that the audit record is protected against modification and destruction; and
- provide means for individuals to check on and correct the information held about them that is used for authentication.

TRUSTe[14] provides tools to increase trust between digital businesses and their customers and has set ten high-level requirements to be considered by every company to protect personal or sensitive data:

- an enterprise-wide data security policy and employee training program;
- internal control over the collection, use and sharing of confidential or private data;
- access procedures based on an individual's ''need to know'';
- internal control over the management of third-party vendor or outsourced relations;
- administrative control and physical security;
- perimeter controls, such as firewalls and VPNs;
- encryption of sensitive data;
- updates for anti-virus software and security patches;
- identity management and authentication procedures (when feasible); and
- regular tests and monitoring.

The AMBIENT AGORAS project (January 2001-December 2003) has also developed privacy design guidelines for systems designers[15].

Trustmarks

A trustmark could be a useful safeguard. One such trustmark is that awarded by TRUSTe which claims to be the most widely used. By posting the trustmark, operators or service providers or others certify that they comply with industry-wide accepted best practice in the collection and storage of any personal or sensitive data they collect.

Liability and insurance

The insurance industry has a role to play in protecting privacy and preventing identity theft. If companies are made liable for breaches in securing their personal data, then they will seek insurance to offset that liability. Before providing such insurance, the insurance companies will want to make sure that prospective clients have taken requisite measures to protect the data they hold.

Media attention

Threats to privacy and identity theft have become important public issues, helped by stories in the press. Reports from the National Academy of Sciences and recent books such as *The Digital Person* (Solove, 2004) and *No Place to Hide* (O'Harrow, 2005) have also served the public interest by documenting how personal information is being abused by both the government and the corporate sector. Such unwanted publicity may be expected to lead to better practice in government and in the private sector in terms of privacy protection.

Organisational measures and consumer awareness

To ensure information security, organisational steps should be taken inside and outside companies to improve awareness and knowledge of employees and consumers about the need to protect personal information, to formulate better security policies and to regularly carry out information security audits.

Conclusions

From the projects, reports and studies reviewed by SWAMI, one can conclude that there is a strong belief in the advance of technology towards an internet of things, with ''intelligence'' embedded everywhere. Indeed, sensors and other devices are already embedded in many things and this trend will undoubtedly continue. While there are many benefits from such technological development – for economic growth, convenience, security, individual and social safety, etc. – there are also growing concerns about threats to privacy, profiling, surveillance, spamming, identity theft (fraud) and so forth.

Safeguards are being developed. Where privacy, identity and security issues have been taken into account in projects, there is generally good recognition that such issues are important to user acceptance of AmI. In an online mode, the user is (sometimes) conscious of the need to make a deliberate decision with regard to appropriate levels of privacy and security. Such will not necessarily (or even likely) be the case in the instance of ambient intelligence. Indeed, an individual may not even be aware that he is in a space embedded with ambient intelligence.

Among the initial principles SWAMI can draw from its review of projects in Europe are the following:

- Privacy considerations should be taken into account and designed in from the start rather than after an AmI technology has been developed or deployed.
- Privacy enhancing technologies should be easy to use and to understand.
- Individuals should be able to specify their privacy preferences.
- Personal data should not be collected unnecessarily (data minimisation).
- In designing any new technology, potential vulnerabilities should be investigated, not only in the technology, but also in the possible cascading or secondary effects that may result from a failure.
- The dependencies between AmI technologies also should be investigated and their consequences for privacy, identity, security, etc.
- The introduction of new security measures should similarly be assessed to determine whether they create insecurities in some other part of the security chain.
- If biometrics are used for identification and authentication, privacy should be considered together with best practices.

- Fixing an identity in one context should not lead to function / mission creep.
- Policy, regulation and technology development should work hand-in-hand and concurrently.
- In consideration of new policies or regulations or alternatives to regulation that may be required as a consequence of the introduction or proliferation of a new technology, impacts should be assessed and stakeholders consulted.
- Policies and regulations should satisfy the interests and concerns of all involved stakeholders as far as possible and to the extent they cannot satisfy some stakeholders, an explanation should be given as to why that is not possible.

Notes

1. See www.privacyrights.org/ar/RFIDposition.htm
2. We adopted the schema of visions, scenarios, roadmaps, research agendas and projects from the diagram on p. 4 of the *Embedded Systems Roadmap* (Eggermont, 2002).
3. www.wireless-world-research.org/general_info/BoV2001-final.pdf The next version of *The Book of Visions* is to be published in spring 2006.
4. www.nri.co.jp/english/opinion/papers/index.html
5. www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2004/2004-index.html
6. PAMPAS is the acronym for Pioneering Advanced Mobile Privacy And Security (www.pampas.eu.org).
7. RAPID is the acronym for Roadmap for Advanced Research in Privacy and Identity Management. Its roadmap is available at http://europa.eu.int/information_society/activities/egovernment_research/documentation/index_en.htm#identity
8. AMSD is the abbreviation for Accompanying Measure System Dependability (https://rami.jrc.it/roadmaps/amsd).
9. The full title of the OZONE project is New Technologies and Services for Emerging Nomadic Societies (www.extra.research.philips.com/euprojects/ozone/).
10. Testimony and Statement for the Record by Shankar Sastry, Chairman, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley. Hearing on ''Cybersecurity: Getting it Right'' Before the Subcommittee on Cybersecurity, Science, Research and Development, Committee on Homeland Security, United States House of Representatives, July 22, 2003 (hsc.house.gov/files/testimony%20Sastry.doc).
11. www.nttdocomo.com/presscenter/pressreleases/press/pressrelease.html?param[no] = 546
12. Symantec Australia Submission to the Parliamentary Joint Committee of Public Accounts and Audit Inquiry into Management and Integrity of Electronic Information in the Commonwealth. The validity of this prediction has not been long in coming. In January 2003, the ''Slammer'' worm spread with such unprecedented speed – it infected more than 300,000 vulnerable Microsoft servers in less than 15 minutes – clogging networks worldwide, crashing bank ATMs and delaying airline flights. See ''Online financial crime headed from bad to worse'' by Brian Krebs, washingtonpost.com, December 17, 2003.
13. The award was announced in April 2005 (www.nsf.gov/news/news_summ.jsp?cntn_id = 103178&org = NSF&from = news).
14. www.truste.org/about/securityguidelines.php
15. The full title of the Ambient Agoras project is Dynamic Information Clouds in a Hybrid World (www.ambient-agoras.org).

References

Borriello, G. *et al.* (2004), *Radio Frequency Identification Technologies: A Workshop Summary*, Committee on Radio Frequency Identification Technologies, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council Of The National Academies, The National Academies Press, Washington, DC.

Dash, E. and Zeller, T. Jr (2005), ''MasterCard says 40 million files put at risk'', *The New York Times*, June 18.

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J. and Burgelman, J.-C. (2001), *Scenarios for Ambient Intelligence in 2010*, final report, IPTS, Seville, available at: www.cordis.lu/ist/istag-reports.htm

Eggermont, L. (Ed.) (2002), *Embedded Systems Roadmap 2002: Vision on Technology for the Future of PROGRESS*, STW Technology Foundation, Utrecht, available at: www.stw.nl/progress/ESroadmap/index.html

Estrin, D. *et al.* (1991), *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers*, Committee on Networked Systems of Embedded Computers, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council, National Academy Press, Washington, DC, available at: http://books.nap.edu/catalog/10193.html

Information Society Technologies Advisory Group (ISTAG) (2002), *Trust, Dependability, Security and Privacy for IST in FP6*, report, Information Society Technologies Advisory Group, Brussels, available at: www.cordis.lu/ist/istag-reports.htm

Information Society Technologies Advisory Group (ISTAG) (2003), *Ambient Intelligence: From Vision to Reality*, Information Society Technologies Advisory Group, Brussels, available at: www.cordis.lu/ist/istag-reports.htm

Information Technology for European Advancement (ITEA) (2004), *ITEA Technology Roadmap for Software-Intensive Systems*, Information Technology for European Advancement, Eindhoven, available at: www.itea-office.org

Ito, M. *et al.* (2003), *Smart Furniture: Improvising Ubiquitous Hot-spot Environment*, Graduate School of Media and Governance, Keio University, Tokyo, available at: www.ht.sfc.keio.ac.jp/~niya/thesis/smart_furniture_iwsawc2003.pdf

Kent, S. and Millett, L. (Eds) (2003), *Who Goes There? Authentication Through the Lens of Privacy*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academies Press, Washington, DC, available at: http://books.nap.edu/catalog/10656.html

Mobile IT Forum (mITF) (2004), *Flying Carpet: Towards the 4th Generation Mobile Communications Systems*, Mobile IT Forum, Tokyo, available at: www.mitf.org

O'Harrow, R. Jr (2005), *No Place to Hide*, Free Press, New York, NY.

Ricadela, A. (2005), ''Sensors everywhere'', *InformationWeek*, January 24, available at: www.informationweek.com/story/showArticle.jhtml?articleID = 57702816&pgno = 2

Schneider, F. (Ed.) (1999), *Trust in Cyberspace*, Committee on Information Systems Trustworthiness, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academies Press, Washington, DC, available at: http://www7.nationalacademies.org/cstb/pub_trust.html

Schneier, B. (2003), *Beyond Fear*, Copernicus Books, New York, NY.

Solove, D. (2004), *The Digital Person*, New York University Press, New York, NY.

Tafazolli, R., Correia, L. and Saarnio, J. (Eds) (2005), *Staying Ahead! Strategic Research Agenda*, eMobility Mobile Communications & Technology Platform, Stockholm, available at: www.emobility.eu.org/research_agenda.html

Wireless World Research Forum (WWRF) (2001), *The Book of Visions 2001 – Visions of the Wireless World*, Wireless World Research Forum, Zurich, available at: www.wireless-world-research.org/general_info/BoV2001-final.pdf