TECHNOLOGY-BASED RESEARCH AGENDA ON THE DATA PROTECTION LAW

Olli Pitkänen

Helsinki Institute for Information Technology HIIT

P.O.Box 9800, 02015 TKK

Finland

olli.pitkanen@hiit.fi

ABSTRACT

This paper discusses legal and ethical privacy issues that scenarios on future information products and services, especially mobile devices, ubiquitous computing, and ambient intelligence technologies arise. First, some general observations of privacy law are presented. Then a few scenarios and examples of future technologies are briefly introduced. Finally, legal and ethical issues that the scenarios bring out are further elaborated. It appears that current data protection legislation does not adequately regulate forthcoming challenges. The quantitative change, namely the increasing number of privacy issues highlights the existing problems in the data protection law, but the qualitative changes, like changing notions, biased laws, as well as new kind of challenges will call for more radical reforms. Therefore issues that need to be studied further to improve the law are concluded.

KEY WORDS

Privacy, Data Protection, Scenarios, Ubiquitous Computing, Ambient Intelligence

1 Introduction

While we are still amid the Internet revolution, the next upheaval by information and communication technology (ICT) is already emerging. It is called ubiquitous computing (*ubicomp*), ambient intelligence (*AmI*), or pervasive computing. Computers are no longer only mainframes, desktop machines, and laptops, but also embedded in mobile phones, vehicles, consumer electronics, toys, and kitchen appliances. Increasingly everything includes microprocessors, memory, communication devices, and software. Already today, a new car easily includes more program code than what is installed in a typical personal computer. This development benefits the users: the digital technology makes vehicles more secure and easier to use, helps people in their everyday life, and provides them with new services.

Context awareness and personalization adjust services to the specific circumstances and needs of a certain person. For example, one probably needs different services while working at the office by the desk and while walking in the street in a holiday. A system that knows about the person's situation and activities can be very helpful not only by providing useful information and services but especially by filtering out those that are unnecessary.

In a few years, all the goods that are produced include Radio Frequency Identification or *RFID* tags, which can store information and communicate via radio frequency with a reader device. RFID is able to identify a product at a distance. That makes the logistics of retail chains much more efficient, helps to improve inventory control, increases security as people and goods are easier to identify, makes it more difficult to counterfeit products, and so on. Also, RFIDs enable new innovative applications: a laundry machine that is able to identify each cloth and adjust the programs for them, or a fridge that knows what is inside and may alert when the "best before" date of a product is approaching. There are lots of useful applications for RFIDs as well as for ubicomp and AmI technologies at large.

On the other hand, many people are concerned that the new technologies increasingly jeopardize privacy. RFIDs make it easy to identify and track people unnoticed. Anyone in the street equipped with a suitable reader may scan what somebody has bought from a shop or what kind of underwear she is wearing. Positioning systems and context aware services provide information on where and with whom someone has been. Personalization usually requires the system to processes personal information. Ubicomp devices gather information on us and transfer it through the networks.

It is difficult to actually foresee how dangerous those threats are. Most people do not seem to care about their privacy in the era of the Internet, so why should they worry in the age of Ami? Does the current legislation give enough protection or should it be changed?

This paper summarizes a study on a number of future scenarios and examples of emerging technologies to analyze the privacy threats, to see if the law needs to be adjusted, and to define what the most important areas to study further in this field are.

2 Privacy

There seem to be a large consensus that developing information and communication technologies are threatening privacy. However, there does not seem to be a consensus on what privacy actually means. Several viewpoints can be taken: at least technological, ethical, and legal. Each of them has many definitions on what is privacy. It is not necessary to present them all here, but a few approaches are described to illustrate the privacy scene.

From the technological point of view, privacy is closely related to secrecy. Typically, privacy is considered to be one's ability to stop information about oneself from becoming known to people other than those whom one chooses to give it. Privacy is also sometimes related to anonymity. [19]

From the ethical point of view, privacy is often divided into several components. *Informational privacy* is a restriction on facts about the person that are unknown or unknowable. It is confidentiality, secrecy, data protection, and control over personal information. *Physical privacy* is a restriction on the ability of others to experience a person through one or more of the five senses. It is spatial seclusion and solitude. *Decisional privacy* is the exclusion of others from decisions, such as health care decisions or marital decisions, made by the person and his group of intimates. *Dispositional privacy* is a restriction on the ability of others to know a person's states of mind. *Proprietary privacy* refers to control over names, likenesses, and repositories of personal identity. [2][17]

According to ALLEN, "the liberal conception of privacy overlaps considerably with the liberal conception of private property. We associate privacy with certain places and things we believe we own, such as our homes, diaries, letters, names, reputations, and body parts. At the core of the liberal conception of privacy is the notion of inaccessibility. Privacy obtains where persons and personal information are, to a degree, inaccessible to others."[2]

Privacy is often considered as an essential element of democratic societies, because it promotes the ideological variety and political discussions. The claim to privacy finds moral justification in the recognition that people need to have control over some matters that intimately relate to them in order to function as people and be responsible for their own actions. A civil society consists of quite autonomous individuals who need a degree of privacy to be able to fulfil the various roles of the citizen in a liberal democratic state. Foremost among these matters that intimately relate to citizens are rights to one's own body. [6][10][17]

What a person is expected to do in order to respect another's privacy varies with culture. According to DECEW, while almost all cultures appear to value privacy, cultures differ in their ways of seeking and obtaining privacy, and probably do differ in the level they value privacy. [6]

According to GOW, "privacy is clearly a value that is important in modern societies and will likely remain so for some time to come. The difficulty lies in establishing a balance between the rights of the community and those of the individual, particularly in the face of new technologies that dramatically increase our ability to collect and use personal information. In many cases, this ability is a desirable innovation to the extent that it can improve the efficiency of governments and businesses, thereby reducing costs to citizens and consumers. On the other hand, such technological developments threaten to sustain a surveillance society involving pervasive data collection from our public lives and unwanted intrusions into our private actions through data mining of our ever-expanding information trails. [10]

It is also interesting that surveys and experiments have uncovered a dichotomy between stated attitudes and actual behavior of individuals facing decisions affecting their privacy and their personal information security. Surveys report that most individuals are concerned about the security of their personal information and are willing to act to protect it. Experiments reveal that very few individuals actually take any action to protect their personal information, even when doing so involves limited costs. [1] In practice people are not that interested in protecting their privacy. Considering that privacy is said to be increasingly in danger, but people still ignore to protect their private information, and some people are even willing to sell the details of their private life to the media, it suggests that the notion of privacy is changing.

Yet another, maybe a little sarcastic, but thought-provoking viewpoint is provided by American legal scientist and philosopher ANITA L. ALLEN. The longish quote below is to even up sometimes a bit overheated privacy-discussion: [3]

"Privacy is still possible, of course. It is still possible to spend an hour alone with a book behind closed doors, an hour in a garden secreted in the corner of a backyard, an hour in bed with a lover. Economic class may determine whether one can buy a book or a garden; gender may determine whether one is nursing as one reads; and religion may determine how guiltless the tryst. But privacy is still possible.

Privacy is also still possible, unfortunately, because the sick die alone in hospital rooms crowded with machines; the seemingly incorrigible languish in solitary prison cells; the vulnerable are harassed and abused at work and in their own homes. Privacy is still possible, though, to some extent, one must wish that privacy were less possible, accountability more exacting. Those who injure

and abuse should he exposed and brought to justice. We need to reexamine institutions and practices that encourage inhumane social isolation."

And further according to ALLEN, there are two peculiar aspects of the end-of-privacy anxiety. [3]

Allen writes: "The first peculiarity is that the anxiety sometimes seems out of proportion to the threat. The affluent occupy 4,000-square-foot homes nestled among mature trees in bucolic suburbs; they work in those homes and in spacious private offices; they drive alone in commodious sedans; they stroll about anonymously in urban centers; they vacation at remote resorts; they date, marry, and divorce whom they please. And yet they decry their loss of privacy. To be sure, the Internet compromises informational privacy, and there are limits on certain important choices (try to marry your lesbian lover in South Carolina). But in the United States, the affluent, and a great chunk of the middle and working classes, have considerable physical privacy and personal autonomy.

The second peculiarity about the anxiety of the age is that all the talk about the involuntary loss of privacy coincides with a good deal of voluntary waiver and alienation of privacy. One wonders sometimes if Americans are losing the taste for privacy. Scarcely any topic, from diseases to divorces, can be discussed at the water cooler. The family secret, on behalf of which Louis Brandeis and Samuel Warren invented the right of privacy, is just another commodity, an eventual disclosure awaiting a lucrative media contract. A hundred years ago a woman might have sued to ease the shame of a stranger witnessing the birth of her child; today she might give birth live on the World Wide Web.

As a culture, we are obsessed with privacy, and so we express outrage when others invade our privacy; but we are equally obsessed with the private, and so we are mass consumers of other people's private lives and willing purveyors of our own." [3]

From the legal point of view, the right to privacy is a human right expressed in several international conventions and a fundamental right stipulated by the constitution of many countries. It is then reflected by national laws.

According to ROBERTSON, the right to privacy is perhaps best understood as combining three related desires or needs:

The *first*, and most readily found in civil rights legislation, is the traditional sense of a private *physical space* the state may not enter except in special cases. The typical protection here is found in restrictions against searches of one's person and possessions, or entry into one's home. The British saying of 'An Englishman's home is his castle' finds echoes everywhere. In the USA, this has been applied to such an extent that a policeman stopping and searching a person on the street and finding the clearest evidence of a crime may not be able to use that evidence if he had no good reason to suspect the person of the crime in question. Even human rights codes like the German Constitution may not spell the right out in much detail; Article 13 starts with the very bald statement: 'Privacy of the home is inviolable'. [21]

A *second* major sense of the right to privacy has become closely intertwined with personal morality, with a strong sense, though little constitutional text backing the sense, that there is a sphere of private activity that the state has no business to regulate. An example is abortion: should an individual have a right to decide to terminate her pregnancy or has the state the power to forbid it. In the USA, the famous case of Roe v. Wade established, in 1973, a fairly unrestricted right to abortion largely on the basis of a constitutionally guaranteed right to privacy. This right, however, cannot be found in so many words anywhere in the Constitution, and is usually defined as a 'penumbral right', one that is implied by other more specifically-stated rights, including the search and seizure type rights mentioned above. Similarly, cases before the European Court of Human Rights concerning abortion have often been founded on Article 8, which provides that "Everyone has the right to respect for his private and family life, his home and his correspondence". In practice the Court has not argued strongly for a right to abortion, and is usually tolerant of the individual states' need for variance on the issue. This is hardly surprising, because Article 8 is itself a very good example of how vague, and in the end how weak, privacy protection tends to be. The second clause of the Article contains one of the widest exception rules, permitting the state to breach this right not only in national security cases, to protect other people's rights, or various other situations one might expect, but 'for the protection of health or morals'. [21]

The *third* concept of privacy that gets some legal protection at times is best demonstrated in relation to religious freedom, which is not only a freedom to practise a religion without hindrance, but can sometimes present itself as a freedom not to be bothered by other people's religious concerns, that is, to have a privacy of belief. This understanding lies behind the very strong US rulings, based on the Supreme Court interpretation of the First Amendment, against the state in any way at all supporting the presence of religion in educational establishments. It is sometimes referred to as 'the right to be left alone'. [21]

Privacy rights are ultimately autonomy rights, the right to act and to develop in one's own way, but there is also a public concern for privacy, the strong sense that it is improper for other people to be nosy. According to ROBERTSON, this is an area where the judiciary in the UK has, until recently, been more cautious than in continental Europe. Since the passing of the Human Rights Act (1998) there have been rulings suggesting that some version of a right against third-party snooping and publishing may be developed. This sense of privacy lies behind the recurrent demands for restriction on, for example, tabloid newspapers printing stories about private

lives. National jurisdictions vary somewhat on this issue, but any strong curtailment of the media in the interests of privacy runs flatly against the better defined and more entrenched rules on freedom of speech. [21]

Privacy is typically related to private surroundings, but wherever an individual is, there can be a justified need for privacy to some degree. The European Court of Human Rights accepts the protection of privacy in the working place, and has introduced the notion of "reasonable expectation of privacy" which applies also to the working sphere.[20]

It should be noted that the right to privacy as a constitutional fundamental right or an international human right is also restricted by other equally important rights, like the freedom of speech, the protection of property, the freedom of trade, and the principle of equality. The fundamental and human rights do not have a general priority order, but if two of them are in conflict in a concrete case, it must be considered, which of them is more important in those circumstances.

3 Data Protection

Most scholars seem to take data protection as a part of privacy protection, while some consider them separate but complementary tools.

DE HERT and GUTWIRTH describe privacy and data protection as two different, but complementary legal tools. Privacy provides opacity, while data protection provides transparency for the data subjects. [13] On the other hand, transparency and opacity may involve in a same privacy case, like for instance, if the freedom of speech, the freedom of press, and public interest requires to disclose certain information (transparency), but privacy does not allow it (opacity). That is a typical case, when somebody claims that a newspaper has violated his or her privacy by publishing some information on private matters, and the newspaper excuses by saying that it was in the interest of public and allowed by the fundamental freedoms to publish the information. In that case, a court needs to weigh the alternatives and decide whether transparency or opacity is more important. However, in privacy and data protection, transparency and opacity that are directed to different objects, are merely the two sides of the same coin. [14]

Europe has been heading the development of the data protection law. Therefore the following concentrates on the European data protection legislation. Similar trends, however, can be found in other countries also.

On the European Union level, data protection is extensively regulated by directives and regulations. For example, Data Protection Directive (95/46/EC) is about the protection of individuals with regard to the processing of personal data and about the free movement of such data, and Directive on Privacy and Electronic Communications (2002/58/EC) applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.

On the other hand, numerous national laws include rules that affect data protection. They may stipulate more in detail and more strictly how personal information is to be handled in certain situations, or they may authorize certain usage of private information more freely than general rules would allow. Privacy is also protected by penal codes. Consequently, the legal construction of data protection rules is quite complex. The rules cannot be found in one law, but they are spread out in numerous statutes.

Data protection law can be applied to a wide area of legal questions. Data Protection Directive applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. If the processing is carried out at least partially by automatic means, the law is applied even to a single personal data item. 'Personal data' on the other hand means any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. 'Processing of personal data' ('processing') means any operation or set of operations, which is performed upon personal data, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Note that if personal data are anonymized in a way that they cannot be related to an identified or identifiable natural person, data protection law is normally not applicable.

The one, who is mostly liable of the possible violations of data protection law, is the 'controller' that is the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data. The one who processes personal data on behalf of the controller is called a 'processor'.

The processing of personal data is not illegal in general. On the contrary, the data protection law tries to enable useful processing of personal data. However, the processing must be carried out in accordance with the law. Especially, data protection directive requires that personal data must be

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

Personal data may be processed only if the data subject has given an unambiguous consent or there is another lawful basis for processing.

If personal data is obtained from the data subject, the controller must provide the data subject at least with the following information:

- the identity of the controller and the possible controller's representative;
- the purposes of the processing for which the data are intended;
- the recipients or categories of recipients of the data;
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- the existence of the right of access to and the right to rectify the data.

On the other hand, where the data have not been obtained from the data subject, the controller must provide the data subject with at least the following information, except where the data subject already has it:

- the identity of the controller and of his representative, if any;
- the purposes of the processing;
- the categories of data concerned,
- the recipients or categories of recipients,
- the existence of the right of access to and the right to rectify the data.

It is also important that disclosing by transmission, disseminating or otherwise making available to others is considered to be the processing of personal data and thus needs also consent or another lawful basis. Especially, transferring personal data outside the European Union is highly restricted.

There are some important restrictions to the applicability of data protection law. Usually, if a natural person in the course of a purely personal or household activity processes personal data, the data protection law is not applied. Furthermore, the data protection law applies only partially to journalistic and artistic context. Also, the law is not always applied to data processing that is related to national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions, as well as to an important economic or financial interest of a Member State or of the European Union.

Completely automated individual decisions are restricted. According to directive, everybody has a right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. However, completely automated individual decisions are allowed, if the decision is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

Certain sensitive information should not be processed at all without special lawful reasons. These special categories of data include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, and data relating to offences, criminal convictions or security measures.

European Court of Justice made an important precedent in *Bodil Lindqvist* case (C-101/01, 2003). The court decided that it constitutes the processing of personal data, if one refers on an internet page to persons and identifies them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies. Such processing of personal data is not covered by the exceptions of the Data Protection Directive. Normally, if a natural person in the course of a purely personal or household activity processes personal data, the data protection law is not applied. However, publishing information in a web page and making personal data accessible to anyone who connects to the Internet causes that it cannot be considered purely personal activity. Thus the data protection law applies to even personal homepages of private people if they include identifiable information on other individuals.

Mobility, context awareness, and ubiquity will bring computer networks even into the most intimate places and walks of life. Future computing and communication devices are not only capable of accessing people's private information but many useful services are highly dependent on it. There will an increasingly important

dilemma: people are requesting and can benefit from services that jeopardize their privacy.

On the other hand, for certain service providers there may be incentives to collect as much private information from people as they can, because that information can be worth a lot of money. Also, it is often more difficult and expensive to build technical systems that secure private information than to ignore privacy needs. Therefore service providers easily disregard privacy unless customers insist upon it or a legal system forces them to honour it.

The recent changes in legal systems, such as European directives on data protection, have substantially improved privacy protection. Some of the chosen actions, however, tighten the privacy requirements in a way which makes it difficult to develop services that users would like to have.

4 Scenarios and technology samples

Compared to traditional jurisprudential research methods, futures research provides us with more suitable means to study forthcoming legal issues. Especially scenarios are useful when we want to describe what the world may be like and what kinds of legal challenges may occur in the future. Scenario-based methods offer a scientific basis for describing the future and evaluating it from the present day perspective.[18]

Scenarios are useful tools for researching future phenomena. They are descriptions of which are possible futures. It must be emphasized that they are not predictions. Instead they are depictions of the future that are useful to clarify our thinking. [18]

I have analyzed a number of scenarios that describe future mobile, ubicomp, and AmI products, services, applications, and use-cases. Many of them highlight privacy and data protection issues. A few examples below describe what kind of topics they expose.

4.1 ISTAG Maria

One of the best known examples of Information and Communication Technologies (ICT) scenarios is the work that the European Commission's IST Advisory Group (ISTAG) has conducted. ISTAG has tried to get a higher level of focus and a higher pace of development in Europe on ICT. As a part of this work, ISTAG launched a scenario planning exercise in 2000. The scenarios were developed by the IPTS (part of the European Commission's Joint Research Centre) in collaboration with DG Information Society and with the active involvement of 35 experts from across Europe. The aim was to describe what living with 'Ambient Intelligence' might be like for ordinary people in 2010. [9]

ISTAG scenarios can be considered quite optimistic – even unrealistic what comes to the pace of technological development. Yet, they present the European vision of high-tech development in the field of ambient intelligence. As they have been produced by the advisory group of European Commission, they also portray the somewhat "official" image of the future. Therefore, even though the scenarios are already a few years old, it has been interesting to analyze them and especially compare them to the requirements that European legislation states.

One of the ISTAG scenarios is *Maria*. It is a scenario about a busy business person from Europe having a business trip to Asia and using highly automated communication systems. Her computing system for the trip is reduced to one highly personalised communications device, her 'P–Com' that she wears on her wrist. From the legal point of view it is notable that most transactions – both private and public – are automated; hardly any human interaction is required. For example, she is able to stroll through immigration without stopping because her P-Com is dealing with the ID checks as she walks. She also gets a rental car and the right to drive to the restricted areas of a city centre, because of a deal negotiated between her personal agent and the transaction agents of the car-rental and hotel chains. The machines make very significant decisions, like they seem to decide who is allowed to enter a country, and they make binding contracts on behalf of someone else.

The context sensitive services utilize a lot of personal information. For example, her hotel room adapts to her 'personality' as she enters.

The ambient intelligence technologies described in Maria scenario represent notable challenges to privacy. The interconnected computing devices must have access to a large amount of private information to be able to provide the services. This might poses severe risks to privacy. The scenario does not refer to any such problems: the system is working perfectly and it honors the users' privacy. Nothing however ensures that. If the system has so much private information about people, it is very easy to – intentionally or by mistake – use it wrongfully or distribute it too widely.

Actually, often the best solutions from the purely technical point of view are unacceptable from privacy perspective. For example, access control mechanisms that prohibit unauthorized use of information are complex to implement and decrease the overall performance and usability of a system. Therefore it is often tempting to leave such mechanisms away or at least make them as light as possible. Unless a paying customer insists or a law requires, a system provider easily ignores privacy protection.

In the European Union, as discussed above, several directives and other statutes have been introduced to protect privacy and personal information. However, the autonomic nature of ubiquitous computing has implications that cannot be adequately addressed by existing legislation. An example of this situation relates to the use of location data to provide essential context for many ambient intelligence services. Processing such location information falls under the provisions of the

directive which requires explicit consent by the user. In an ambient intelligence environment where a number of services by different service providers are used in tandem it is difficult to notify and receive the consent of users to process location data every time this is necessary.

In fact, the directive requires that the user accepts separately the use by each service of their data and even more, services must provide continually the "possibility, [of] using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication."

Indeed, it appears that this aspect of the directive completely excludes the possibility of federated service provision. Moreover, if users are required to accept separately the use of their private data by each service then in practice, it is most likely that users simply would not use the services rather than accept this management overhead. Surely, usability improvements and automatic mechanisms can make the situation much easier, but ultimately the user must have control and the ability to refuse the processing of location data in order to fulfill the requirements of the directive. Finally, while the directive aims to harmonize legal systems and guarantee certain level of protection within the EU, obviously it does not apply in countries outside its boundaries.

In *Maria* scenario for instance, it seems that many services would benefit from her location data. However, the situation becomes very complex if Maria needs to accept separately each service to use the data, and each service must provide her with the continuing "possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication". In practice, it would probably be easier for Maria simply not to use the services. Surely, usability studies and automatic mechanisms can make the situation much easier, but ultimately the user must have control and the ability to refuse the processing of location data in order to fulfill the requirements of the directive.

The directives aim at harmonizing legal systems and guarantee certain level of protection within the EU, but obviously they do not apply in countries outside the Union. Therefore, exchanging information within the Union has been tried to make flexible. On the other hand, it is highly restricted to transfer personal data from the member countries to "unsafe" countries outside the EU.

In *Maria* scenario, European citizen is traveling outside Europe. Her personal data mainly originate from the Union but is needed in Asia. Presumably Maria is willing to use those personalized services and therefore accepts the transfer of her personal data between at least her home-country and the Asian country. Yet, in accordance with the directives and European national laws, she has to explicitly accept the transfer of data from Europe to the Asian country. This effectively protects her privacy, but introduces severe challenges to the designers of the services. Also, it decreases the efficiency of the concept that was emphasized by ISTAG. According to ISTAG, "Ambient Intelligence works in a seamless, unobtrusive and often invisible way." The need to get consent from the user makes this goal hard to achieve.

4.2 Between Scenarios

In HIIT's Between project the idea of ubiquitous computing was investigated from the user's point of view by creating user scenarios and experience prototypes with user-centered product concept design methods. The emphasis was on mobile ubicomp. The project created the total of 48 scenarios. Eight of them were further elaborated, and finally two prototypes were developed based on five of those eight scenarios. [15]

Below, the eight scenarios are described as examples of emerging technologies.

Ubiquitous SIGs (01-6): Individuals belong to different special interest groups (SIG). SIGs are tagged with location-dependent and -independent services and information. SIGs activate and become visible when members enter a cell. Push-services are listed separately from the activities organized and activated by the members.

Give me a break! Mode-based filtering (02-1): Context-sensitive push messages are filtered according to modes that are switched on/off either manually or automatically. Others can view the mode you're in. "Meeting is over and Risto heads for lunch. Risto switches to 'Break' mode. Having made his order, Risto sits down. He notes that the restaurant provides jokes for his break. Risto skims through some of the jokes. As Risto returns to the office, the magic thing announces mode switch with barely perceivable haptic stimulus."

Silent push (02-3): Niina is at Esplanade, she is in a hurry going to her friend in Katajanokka. There is an event with a band and a lot of people, but she does not have time to stop there this time. Her magic thing is in her pocket, silently displaying what is going on in that area. When she moves on further away, this information is automatically erased.

Coffee mug (04-1): Tero is editing three articles for the next issue of his computer magazine Datalehti. He is in hurry to edit all those articles. He decides to talk with his colleagues who could help him. He stands up from his desk and heads towards the kitchen at the other end of the office. As he takes his coffee mug with him, the coffee mug automatically downloads all the three Word documents currently active or open on Tero's personal computer and beeps three times at a barely audible volume. Tero walks to the kitchen and pours some coffee to his mug. He then walks to Jenni's desk and asks if she could edit the Cruz Broker story.

The Event Tagging Device ("a knot in your finger") (04-2): Erno and Jussi are having a coffee break at the office.

Among other things they are discussing about an article Erno is writing. They agree to meet on Thursday and Jussi promises to forward some related email to him before that. Erno does not have his calendar with him, so he tags the event using his Event Tagging Device. The device is small and it has only one button. The Event Tagging Device records all the contextual variables it has access to at a time when the button is pressed (e.g. "Tag 10:30; Location: Coffee Corner; Duration: 17 minutes; Background noise level: low; Present: Jussi, Paula; Devices: JussiPDA, Laserjet 4M"). When returning to his PC, Erno sees list of events he has tagged. Getting a notification from his coffee break with Jussi helps him to remember what he promised to do.

Track Detector (05-5): Standing outside Stockmann, Pirre gets a notification that that Carl-Johan has just been there. Pirre follows Carl-Johan's trace to railway station and they decide to go to café NetCup.

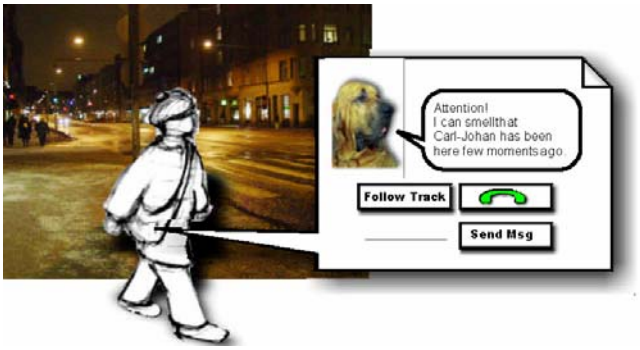

Figure 1. Between scenario 05-5 [15]

Public votes (07-2): Public, location-based votes that everyone can create. "Lili walks by the statue called Kolmen sepän patsas, which is under renovation. She notices that there's a voting. 'Should they put shorts on these naked men? By: [Anonymous182] 89 % No – 11 % Yes.' She votes "No", and continues."

Figure 2. Between scenario 07-2 [15]

Item reminder (09-1): Liisa is leaving home. She has a Magic Thing with her that knows what items she usually carries with her. The Magic Thing notifies her that she forgot her bus ticket and also the probability of needing a lipstick is 68 %. Liisa takes the bus ticket and the lipstick with her. A Bayes-network has learned what items she usually carries with her when leaving home at a specific time and/or in relation to the forthcoming events she has marked in her diary.

The other forty scenarios present ubicomp applications from restaurant watcher to friendship manager. They are strongly focused on people's everyday situations at home, at work, shopping, and in free time. All the scenarios are very small, like flashes on the future. Each of them focuses strictly on a certain single idea on how the future ubicomp technologies help ordinary people in their everyday life. They do not discuss business models or revenue logics.

Between scenarios are quite brief. In the legal analysis, I am trying to stay within the wordings of the original scenarios and not to speculate what else could have been described. Therefore also my analysis stays quite concise.

Between scenarios describe very human centric and personal situations. They intend to bring up future product concepts that help people in their every-day situations based on the needs and experiences of individuals. Therefore, from the legal point of view, they highlight privacy and data protection issues. Most of them present situations in which people are sharing their private information, like information on their location, profiles, belongings, or interests, or even 3D models of themselves, with all the other people around. Only a few scenarios explicitly tell that the users are able to district others' access to information (e.g. 01-5: "Sanna and her friends have made their product ID-tags visible to others as part of their public profile.") while most scenarios imply that anybody can access users' private information (e.g. 02-1: "Others can view the mode you're in.") or ignore the issue.

Probably most of the scenarios could be implemented in a way that users' privacy remains protected. That would however make the technology remarkably more complicated. The scenarios clearly show how easy it is to ignore data protection. Many exciting inventions are possible, if private information is available. Yet, those inventions also enable evil usages. If data protection excludes some of the most thrilling possibilities, it also disables severe misuses of private information.

4.3 Cyborg

One well-known example of emerging technologies that surely have affects on privacy is Professor KEVIN WARWICK's Cyborg project. He carries out research in artificial intelligence, control, robotics and biomedical engineering at the University of Reading. He has shown how the use of implant technology is rapidly diminishing the distance between humans and intelligent networks. In effect as a human is wired in to the network they become a part of that ambience themselves. This can have a tremendous impact in the treatment of different neural illnesses. There is a number of areas in which such

technology has already had a profound effect, a key element being the need for a clear interface linking the human brain directly with a computer.

WARWICK's own research has led to him receiving a neural implant which linked his nervous system bi-directionally with the internet. With this in place neural signals were transmitted to various technological devices to directly control them, in some cases via the internet, and feedback to the brain was obtained from such as the fingertips of a robot hand, ultrasonic (extra) sensory input and neural signals directly from another human's nervous system.

This example shows how the emerging technologies no longer jeopardize only our private information, but also other components of privacy, like physical and decisional privacy as implants and computerized systems are able to affect our nervous systems.

4.4 Further examples

I have also analyzed a number of other scenarios and examples of forthcoming technologies. Most of them present some sort of privacy issues – not very unlike from those above. Therefore, I am quite confident to claim that the examples above represent rather well the view that we are able to have currently on the privacy and data protection issues related to forthcoming mobile, ubicomp, and AmI technologies. [18][19]

5 Conclusion

Computing and communication devices are spreading everywhere in our society. In the future, those devices will become increasingly embedded in everyday objects and places, while communications networks connect the devices together and become available anywhere and anytime. It can be seen partly as a parallel ongoing development with mobile technologies, partly as a successor to them.

According to ISTAG: "in the physical world, domicile and residence are carefully developed and recognised concepts in terms of privacy and security protection in its broadest sense - legal, social, economic and technological. In contrast with the real world, there are few social and legal indicators of what constitutes a protected private space or an open public space in the virtual world. A comparable level of sophistication is needed in the future for people to feel at home within their smart homes, with their online activities, and facilitate the personalisation of their everyday environment in order to enhance their mobility."

How are ubicomp or AmI technologies going to affect privacy? It seems obvious that, because devices that are able to exchange information on people are spreading, the quantity of privacy problems will arise. The scenarios above illustrate that very well. All of the scenarios include a number of privacy issues. Although privacy problems are not that common today, the scenarios suggest that they will be increasingly ordinary.

But will there be also something else? Will some qualitative changes also be likely?

At least three categories of qualitative transforms seem probable. *First*, current legislation, although it claims to be technology neutral, is somewhat biased towards existing technical solutions, like personal computers, large displays, keyboards, and web pages. For example, as discussed above, services must provide continually the possibility, of using a simple means and free of charge, of temporarily refusing the processing of certain personal data for each connection to the network or for each transmission of a communication. It would be quite easy to fulfill such requirements with a PC based system, but very difficult with a tiny ubicomp device which has a minimal user interface.

Second, people's notion on privacy is changing. We are already getting used to the idea that while we are using for instance Internet services, someone can be able to observe our doings. Hardly anybody is worried that vehicles have register plates that visibly identify them. While travelling abroad, we need to frequently present our passports and other documents, even though it makes it possible for authorities to follow our paths. In the past, that was not possible, but still most people are not concerned about the change. The war against terrorism, on the other hand, is accustoming people to diminishing privacy rights for security reasons. Either they accept the reduction of their privacy, because they think it is necessary or that they get something valuable instead, or they do not care. Anyway, it seems likely that most people will not object the gradual impairment of their privacy. In the future people will have a different notion on privacy and they will be happy with that.

Third, information and communication technologies will no longer affect only informational privacy, but increasingly also other sectors of privacy. Professor WARWICK's examples show how the technology can also be used to observe and control the human being through the computer networks from distance. It is possible to even affect his brain's decision-making process. Until now, the developing information and communication technology has threaten only informational privacy. These examples nevertheless clearly show that the emerging technologies are not that limited: they are also capable of jeopardizing the other components of privacy. This implies a major qualitative change in privacy problems.

I conclude that emerging technologies are changing the privacy scheme. The fact that ubiquitous and pervasive computing devices and ambient intelligence technologies are spreading everywhere implies that the number of privacy issues will increase. Consequently, the shortcomings of the current privacy and data protection law will become more apparent. In contrast, the contradiction between technology biased laws and new technologies on one hand, and the changing notion of privacy on the other hand may require more prominent changes in law. And finally, implants and other

technologies that not only gather information on us, but can actually affect us physically, call for a rethink on the legal area. Before these changes can be implemented, further studies need to produce adequate background information for the legislators. This defines the research agenda on the future data protection law.

References

[1] Acquisti, A., Grossklags, J. *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting.* In J. Camp, S. Lewis (eds.) The Economics of Information Security, Kluwer Academic Publishers, 2004.

[2] Allen, A. L. *Coercing privacy*. William and Mary Law Review, 3/1/1999.

[3] Allen, A. L. *Is Privacy Now Possible? A Brief History of an Obsession.* Social Research, Vol. 68 Issue 1, 2001.

[4] Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F., Rohs, M. *Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing*. In W. Weber, J. Rabaey, E. Aarts (Eds.): Ambient Intelligence, Springer-Verlag, 2005.

[5] *Convention for the Protection of Human Rights and Fundamental Freedoms*, the Council of Europe, as it has been amended by Protocol No. 11, 2003.

[6] DeCew, Judith. Privacy. In Zalta, Edward N. (ed.) *The Stanford Encyclopedia of Philosophy* (Summer 2002 Edition), http://plato.stanford.edu/archives/sum2002/entries/privacy/, 2002.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002.

[9] Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J-C. (eds.). *ISTAG Scenarios for Ambient Intelligence in 2010*, Final Report, IPTS-Seville, 2001.

[10] Gow, G. A. *Privacy and Ubiquitous Network Societies*. International Telecommunication Union, ITU Workshop on Ubiquitous Network Societies, Document UNS/05, 2005.

[11] Gutwirth, P. *Privacy and the Information Age*. Rowman & Littlefield, 2002.

[12] Gutwirth, S., De Hert, P., Moscibroda, A., Schreurs, W. *The legal aspects of the SWAMI project*. In: Friedewald, M., Wright, D. Safeguards in a World of Ambient Intelligence (SWAMI), Deliverable D5, Report on the Final Conference, Brussels, 21-22 March 2006.

[13] De Hert, P., Gutwirth, S. *Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence*. In: Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), Institute for Prospective Technological Studies (IPTS), Technical report, EUR 20823 EN, 2003.

[14] Introna, L. D., Pouloudi, A. *Privacy in the information age: Stakeholders, interests and values.* Journal of Business Ethics, Oct 1999.

[15] Kankainen, A., Kankainen, T., Blom, J. *Between - Ubiquitous Bubbles Enhancing Human-Human and Human-Computer Interaction*. Final report, 15.5.2003, Helsinki Institute for Information Technology HIIT, 2003.

[16] Lessig, L. *Code and Other Laws of Cyberspace*. Basic Books, 1999.

[17] The Online Ethics Center Glossary, http://onlineethics.org/glossary.html, 2006.

[18] Pitkänen, O. *Legal Challenges to Future Information Businesses*, HIIT Publications 2006-1, Helsinki Institute for Information Technology HIIT, 2006.

[19] Pitkänen, O. *Legal and Regulation Framework Specification: Competence within Mobile Families and Ad-hoc Communities*, IST-2004-511607 MobiLife, D11 (D1.6) v1.0, 2006.

[20] Punie, Y., Delaitre, S., Maghiros, I., Wright, D., Alahuhta, P., De Hert, P., Friedewald, M., Gutwirth, S., Lindner, R., Moscibroda, A., Schreurs, W., Verlinden, M., Vildjiounaite, E. *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*. Safeguards in a World of Ambient Intelligence (SWAMI). Deliverable D2. A report of the SWAMI consortium to the European Commission under contract 006507. 2006.

[21] Robertson, David. *A Dictionary of Human Rights*. Europa Publications, Taylor & Francis Group, 2nd edition, 2004.

[22] Warwick, K. *Wiring in Humans. Advantages and problems as humans become part of the machine network via implants*. Presentation in SWAMI Final Conference in Brussels, 21-22 March, 2006. Summary of the presentation in Friedewald, Michael – Wright, David. Safeguards in a World of Ambient Intelligence (SWAMI), Deliverable D5, Report on the Final Conference, Brussels, 21-22 March 2006.