ICT and Privacy in Europe

Experiences from technology assessment of ICT and Privacy in seven different European countries

Final report October 16 2006

EPTA

European Parliamentary Technology Assessment

The conclusions in this report are the responsibility of the following six members of the European Parliamentary Technology Assessment network (EPTA):

The Danish board of Technology,
Denmark

Contact: Lars Klüver
www.tekno.dk

Flemish Institute for Science and Technology,
Flanders

Contact: Robby Berloznik
www.vitwa.be

Institute of Technology Assessment,
Austria

Contact: Walter Peissl
www.oeaw.ac.at/ita

The Norwegian Board of Technology,
Norway

Contact: Tore Tennøe
www.teknologiradet.no

Parliamentary office of Science and Technology,
UK

Contact: David Cope
www.parliament.uk/post/home.htm

TA-SWISS – Center for Technology Assessment,
Switzerland

Contact: Sergio Bellucci
www.ta-swiss.ch

Table of Contents **page**

Preface

This report is offered by the European Parliamentary Technology Assessment network (EPTA) as a contribution to the European debate and policy-making on privacy.

It is based on 28 technology assessment projects carried out by the participating EPTA members. These projects have been reviewed and a cross-European synthesis has been made. From the analysis of the societal as well as technological developments we have derived conclusions and policy options.

The EPTA Privacy Project was managed by:

Lars Klüver, director of the Danish Board of Technology
Walter Peissl, senior researcher at the Institute for Technology Assessment, Austria
Tore Tennøe, director of the Norwegian Board of Technology

Besides the management group, the project group consisted of:

Danielle Bütschi	Centre for Technology Assessment, Switzerland
Johan Cas	Institute for Technology Assessment, Autria
Robby Deboelpaep	Flemish Institute for Science and Technology Assessment
Christine Hafskjold	The Norwegian Board of Technology
Ida Leisner	The Danish Board of Technology
Chandrika Nath	Parliamentary Office for Science and Technology, UK
Janus Sandsgaard	The Danish Board of Technology
Stef Steyaert	Flemish Institute for Science and Technology Assessment
Nicole Vouilloz	Centre for Technology Assessment, Switzerland

Rinie van Est of the Rathenau Institute in the Netherlands contributed in the early stages of the project.

The project participants would also like to thank John Borking, Birgitte Kofoed Olesen, Jo Steyaert, Per Helge Sørensen and Susanne Lace for their valuable contribution to the process.

A draft version of this report has been discussed within the director group of EPTA. However, the analysis and conclusions in the report are the sole responsibility of the six participating institutions. It is our hope that this report will contribute constructively to the policy-making on this important issue.

On behalf of EPTA and the project group,

Lars Klüver Walter Peissl Tore Tennøe

Executive Summary

This study builds on experiences from technology assessment of ICT and Privacy in seven different European countries.

Privacy is an important democratic right. In this report we identify five areas that affect privacy: Security, access to information and services, societal interaction, convenience and economic benefit. In addition, we discuss two other fields of public interest where the use of ICTs may be conflicting with privacy, namely e-government and e-health. All these areas are subject to rapid change, and in addition to looking at the challenges today, we also try to describe some future trends that may affect privacy.

Dealing with privacy in terms of trade-offs helps to illustrate that a balance has to be found between conflicting societal values and rights. Our analysis points to some important challenges and corresponding policy options:

Review of surveillance systems by independent body
An important task for governments is to provide their citizens with a high level of security. However, they need to consider whether more surveillance is justified.

It is important that surveillance systems are properly assessed. Their value depends on them being effective, not easily circumvented and resulting in a real security benefit. One option is periodical review of surveillance systems by an independent publicly accountable body.

Citizens' access to their own records and logs
eGovernment increases the flow of information between different public units, in order to provide desired services. It has the potential to dramatically increase the amount of personal information officials hold about citizens.

A vital challenge is how the technology can be used not only to increase efficiency for the public administration; but also to strengthen privacy for the citizen. Governments could consider a mutually transparent system that gives citizens access to their own records and logs, and allows them actively to control the flow of their own personal data.

Empowering data protection agencies
The mandate of data protection agencies remains weak in many countries. As long as ignoring data protection rules bear no consequence, there will be no incentive for industries and public bodies to incorporate privacy principles into their IT systems and services.

A crucial question is the capacity of these agencies to handle complaints in due time. Governments may need to consider seriously whether data protection agencies should be able to proactively conduct investigations, impose effective penalties and monitor the activities of public and private organisations and their approach to data management.

Mandatory privacy impact assessments

The study shows that privacy threats could often be avoided if data protection concerns were built into information systems development from the start. Mandatory Privacy Impact Assessments (PIAs) can contribute to ensuring that privacy is taken into consideration.

In the public sector, PIAs could become a prerequisite for IT project procurement. Although they will involve financial costs, the benefits may be significant. It is cheaper to include privacy concerns in the design phase of systems than to make them privacy compliant at a later stage.

Privacy enhancing technologies (PETs) could be systematically integrated into systems development. An important PET principle is that systems should only collect data on a *need to know* – not a *nice to know* – basis. Delivering services without collecting excess data is cost-effective as well as socially desirable.

International privacy standards can enhance consumer trust and promote equal privacy protection worldwide; and they encourage corporate response.

There is a rapid development of e-services and a new security situation. New technologies such as RFID, biometrics and pervasive computing are also developing rapidly and thus create new possibilities and threats.

This report shows that the value of privacy is underestimated by citizens, policy makers and enterprises. It concludes that there is need for more research on mid- and long-term effects of weakened privacy, and more public dialogue is needed on these issues.

Chapter 1 Introduction

This report on *ICT and Privacy in Europe* is the product of a joint-project of six EPTA member institutions. EPTA is a network of *European Parliamentary Technology Assessment* institutions across Europe. Its 17 members perform science and technology assessment (TA) studies in order to advise parliaments on the possible social, economic and environmental impact of new technologies.

Such work, pioneered in the 1970s by the Office of Technology Assessment (OTA) of the US Congress, is seen as an aid to the democratic control of scientific and technological innovations. The participating institutions are constitutionally and methodologically heterogeneous, but share a concern for providing impartial and high quality accounts and reports of developments in science and technology issues and industrial and R&D policy.

The main purpose of this study is to reach decision-makers on the European and national level in order to provide them with options to face the highlighted challenges to privacy, which originate from technological as well as societal and political development.

1.1 Why is privacy a European policy-issue?

Privacy is a fundamental right and a societal value that is protected on a higher level than other individual rights. In recent years, this pillar of open societies has been challenged by different developments. First, political actions regarding the “war on terror” lead to erosion of some safeguards of privacy. Secondly, the overall goals of rationalisation in public administration lead to systems of e-government and e-health that have the potential to make citizens and patients transparent and intrude privacy. Thirdly, private enterprises look at personal data as an economic resource. With individually addressed target-group oriented marketing they try to gain profit and competitive advantages. And finally technological development also leads to erosion of privacy. Many devices work digitally, they are getting smaller and are more intensively interconnected.

In a short-term perspective, a loss of privacy might lead to an adapted form of behaviour that individuals think they are supposed to show. This is critical because liberal democratic societies are built on the idea of self-conscious and autonomous citizens. In the long run, such a “mainstreaming” of citizens' behaviour, may turn out to prevent the dissenting behaviour that is considered to be an important impulse for economic and societal development

The findings in this report indicate that the development in technological, political, economical and cultural spheres may lead to a society where individual freedom could be seriously reduced unless no measures are taken to prevent this.

1.2 EPTA and the privacy issue

EPTA, as a cross-European network of parliamentary technology assessment institutions, acknowledge our responsibility to contribute with our policy analysis across nations and at the European level. There certainly are important issues related to technology that need such cross-national scrutiny, and EPTA has an important role to play in this. Privacy stood out as one such issue. It is of increasing importance and of fundamental relevance to open democracies, yet awareness of threats to privacy is low. In this study we have synthesised findings from 28 projects conducted by the six partners (see Appendix C for a full overview of the projects). From the analysis of the societal as well as technological developments we have derived conclusions and policy options.

Privacy is an issue that could benefit from being addressed at a European level. Many EPTA-organisations have done work in this field and synthesising the different approaches and results gives insight into common views and values as well as the particularities of different cultures and political systems. Privacy is a European issue where there is a lot of experience gathered in national projects. Integrating these findings will provide added value and in the end be more valuable than just the sum of the parts. Although national legal regulation exists, basic guidelines are discussed and designed at a European level. New challenges will also have to be discussed at a European level, and EPTA wishes to contribute to this discussion.

1.3 Methodology

This project is the result of the close co-operation between staff members in the six participating EPTA institutions. A total of 28 projects conducted by these institutions over the last years have been reviewed, offering a broad cross-European knowledge base on privacy issues.

Each institution has provided reviews of their projects in a common English template, to ensure that all participants can understand and discuss the results of the total project portfolio. The different institutions have looked at many different aspects of privacy, and also used different methodologies in their approach to the issue. A brief description of the different methods used can be found in Appendix B.

After reviewing all the projects, the group decided to focus on 8 themes. The responsibility of each theme was then assigned to different author groups. These groups have worked on drafting, reviewing and finalising each chapter. The full report, and the conclusions and policy options have later been reviewed by all the participants in the project.

Five experts on privacy were invited to a workshop to discuss the policy options derived from the different chapters of the report.

A draft of the report has also been discussed within the director group of EPTA. However, the group of participating institutions is fully responsible for the analysis and conclusions in the report.

1.4 The structure of the report

This report identifies five important trade-offs that affect privacy. In addition, two major fields of public interest where the use of ICTs may conflict with privacy are discussed.

The first part of this report gives an overview of basic trends and technological developments which have major impacts on privacy, such as mobile services, the Internet, pervasive computing and Privacy Enhancing Technologies (PETs). Subsequently a chapter on legislation follows. We sketch out a rough picture on legal developments with specific emphasis on the European situation.

The terrorist attacks of September 11th 2001 gave rise to a political discussion on societal security. Chapter 4 describes different security technologies and how they affect privacy. Politicians are concerned about security threats and citizens want to be protected. Security is often assumed to be synonymous with surveillance. Whether or not security is really enhanced with more surveillance is also a matter of discussion.

Chapter 5 deals with access: We face an increasingly digitalized world. If one wants to be part of modern life one has to use electronic/digital equipment. The loss of privacy to gain access to information and services is often a result of a lack of privacy enhancing design of the ICT systems. The use of PETs could remove or at least mitigate the loss of privacy.

New ICTs create new ways of societal interaction, and in Chapter 6 we discuss how this may affect privacy. When the interaction is digital, it produces a lot of data traces. Total confidentiality could exclude people from social networks, but total exposure could have impact on the privacy of the individual. A choice needs to be made somewhere in the middle, between gaining easy access on the one hand, and giving up personal data on the other.

Why have some technologies become such a success? It is because they add significantly to the convenience of their users. In Chapter 7 we see that these technologies also have a major impact on their users' privacy. The flexible privacy concept in existing legislation reflects this need to continuously negotiate and stipulate privacy requirements. However a strong regulatory basis is needed to guarantee the individual's free choice on the trade-off.

In Chapter 8 we discuss how the need for economic benefit may be a threat to privacy. Enterprises use ICTs because of their potential to raise efficiency and productivity, and they gather customer data for research and marketing purposes. But personal information can also be seen as a resource for the consumer: In consumer cards systems and other electronic discount-systems even consumers gain an economic benefit – if they are willing to sell part of their privacy. In the future it may become important for companies that wish to be perceived as trustworthy to have a clear privacy policy and uphold it.

E-government is a rapidly developing area, and is the focus for Chapter 9. Objectives of most of the e-government projects around the world are saving public money by increasing the efficiency of the bureaucratic system, getting closer to the citizens and delivering a better service to the citizens. The implementation of such systems raises questions concerning privacy.

In Chapter 10 we discuss different aspects of e-health. The most sensitive area where data are concerned is the use of data in the health care sector. The more applications in health care supported by digital equipment, the more questions concerning privacy will arise. In most countries specific laws guarantee confidentiality on the part of health care professionals. This higher level of security must be implemented in techno-organisational systems too.

Chapter 11 – Conclusions and policy options summarises the challenges and presents policy options to meet these challenges both at a national and European level.

Chapter 2 Technologies that affect privacy

By Johann Cas (ITA)

This introductory chapter deals with the impacts of technical developments in ICTs on privacy, i.e. with ways by which technical progress can actually or potentially either threaten or enhance privacy. This brief overview does not address any of the manifold benefits of ICTs on an individual or societal level but rather focuses on privacy effects only. It is these developments that provide the rationale for the individual projects on privacy and ICT carried out by the different EPTA-Members.

Major milestones in technical progress in ICT show serious privacy impacts. Among these are:

- The digitalisation of telecommunications, allowing the generation of communications profiles,
- the rapid diffusion of mobile communications, enriching these profiles by location data,
- the extension of Internet into the daily life of many people, revealing information about personal interests and predilections through the use of its services.

These technological developments are already radically changing the status of privacy by automatically generating huge amounts of data, most of which can be attributed to specific people. These changes are radical in a qualitative manner too; they allow for previously inconceivable and unreachable levels of analysis if no legal or technical provisions are taken to prevent the storage and combination of these data. Further milestones, marking the impending evolution into a panoptic society, are ubiquitous information technologies, improved biometric identification methods or extensive genetic testing.

New technologies do not necessarily determine societal development, and they also provide powerful means of protection of privacy in the form of Privacy Enhancing Technologies (PETs). There is, however, no indication that privacy threatening and privacy enhancing capabilities are being balanced in an automatic manner, on the contrary, without specific policies developed and measures taken privacy intrusive applications and features will continue to dominate over privacy strengthening measures. A major aim of this brief introduction is to raise awareness about potential privacy threats resulting from technological developments and to induce broad

discussions on these issues, hence contributing to rational decision making and policy formation.

This chapter discusses general technological trends of relevance for privacy. More details on specific technologies can be found in the chapters where they are relevant or in Appendix A – Overview of Technologies.

2.1 Digitalisation

A first, crucial step was made with the digitalisation of telecommunications technology. Old detective movies remind us how difficult it was to detect a caller in the age of analogous switches. All sorts of tricks were applied to keep the caller talking long enough to be able to retrace the origin of the call. Electromechanical switches put the connection through digit by digit; when the phone was hung up, the switches returned into the starting position and data on the just finished call was lost. In modern digital networks any call, regardless of whether it is successful or not, generates a data record including the telephone numbers of the dialler and receiver, the time and, if a connection has been established, the duration of the call. Although the generation of a data record does not allow statements about the duration of storage or the use of these data, it implies that an additional step is required to delete these data.

Two factors influenced how long traffic data was stored for: On the one hand, storage capacity cost money and limits were set for economical reasons alone. These reasons are, however, becoming less relevant as costs of storage capacity are rapidly decreasing and more efficient methods of data analysis promise to extract valuable information from what has previously been regarded as data garbage. On the other hand, data protection regulations limited[1] the scope for storing or processing personal or personally identifiable data in a legal manner. Regulations for telecommunications traffic data normally stipulated the removal of those parts of the data records which would show the relation to a natural person, as soon as these data were not anymore required for delivering the service or for billing purposes. For individually billed services – still common for telephone calls – the deadline for filing an appeal also terminated the permission to store these data; for services with flat rates – frequently applied for broad band Internet access – the storage of personal data was prohibited altogether.

2.2 Mobile Services

The rapid diffusion of mobile communications is a further techno-economic innovation with far reaching consequences for privacy. In order to be able to establish communication links to mobile terminals, the terminals' positions need to be scanned

[1] The use of past tense should indicate that the legal situation is changing rapidly (see next Chapter).

and entered in corresponding registers. If a call is initiated, the current position of the mobile device is read from these registers and a connection to the appropriate base station established. For the users of mobile services this means that their location is permanently monitored as long as they carry a switched-on terminal with them. Normally this position-fixing is not very precise; depending whether the user is located in an urban or rural area the accuracy varies between a few hundred meters and a few kilometres. However, from a technical point of view there are no limits to precision. With technical upgrades the position can be determined very accurately on the basis of the delay times of the signal to individual base stations. In addition, a widespread integration of GPS-modules into mobile equipment has to be expected in the future. The ability to identify someone's exact location not only increases the potential to offer advanced emergency assistance and other useful and/or profitable so-called Location Based Services (LBS) but it also creates and reinforces threats to privacy.

Threats to privacy may occur on different levels. A single detail can represent a deep and severe invasion of privacy, e.g. if the factual location does not correspond with the location given to a family member or employer. The possibility of being controlled as such is sufficient for a severe loss in personal autonomy, regardless whether such surveillance is actually taking place or not. If a private person or a company want to locate someone, the consent of the person to be located will normally be required.

If these data are retained, the threats are enlarged by new dimensions. The vague chance that a person is confronted with a location request at a certain point in time is replaced by the certainty that location data is continuously recorded. With the extension of the allowed period of data retention, the information that can be extracted from the data gains a new quality, going far beyond the simple fact of knowing the location of a certain person at a certain time. Even with low precision the daily routines and personal habits of the concerned persons can easily be outlined. If the precision increases, the possibility to draw conclusions from the location data grows correspondingly. By matching the location profiles of different persons, social contacts between groups of people could be made visible; hence the possibility that data analysis, in the past limited to telecommunications based contacts, could be extended to all spheres of life.

Currently the registration and storage of location data is normally limited to the level of radio cells; more exact positioning only takes place if the services ordered require more precision or if surveillance measures are carried out. The conditions could, however, change rapidly. For a broad range of LBS the required technical preconditions need to be created. It can in all probability be expected that the current endeavours to establish obligatory data retention will be extended to this data pool as soon as it is available.

The rapid spreading of mobile information services and terminals has also a direct impact on the character of the data generated with their use. In contrast to fixed equipment, which can be used by a greater number of persons within a household or company and thus offers at least a minimal degree of pseudonymity, mobile equipment is usually used by one individual only. Patterns from the use of such equipment are therefore considerably better suited for the generation of personal profiles.

2.3 Internet

Traffic and location data leave traces about communications that have taken place and locations that have been visited. However, the contents of these communications or the purpose of the presence at a certain place remain in general unknown. When using Internet services these gaps can largely be closed and what has been the exception may become the rule.

In e-mails content and address information are transmitted jointly; as long as the contents are not encrypted they can be compared to a postcard that can be read by anyone that comes across it on the way from the sender to the recipient. A substantial difference is the digital form of the information, allowing automated storage or analysis of the content; e.g. the scanning of messages for certain keywords.

In postings to newsgroups the publication of the message is the objective of the service, for instance to disseminate own points of view or to ask the community for solutions for certain problems. What many don't know is that such messages can be stored for decades – Google Groups reaches back into 1981 – a practice that can be seen as a threat to privacy. The original posting seemingly only survives for a few days or weeks, depending on the level of activity within the concerned newsgroup, but it remains accessible from the archives as long as no active effort is made to delete it.

Most users were and still are unaware of the long term storage of their contributions. This fact arose as a matter of discussion only when it became known that job applicants were scanned on the Internet for information on their personal interests and attitudes. Thereby statements, that have been made under the assumption that they would exist for a short period of time or under circumstances that since have changed, can be taken out of context and interpreted in a disadvantageous way. In the past cautious users could avoid such explorations by using pseudonyms. Should the plans for general data retention, including Internet traffic, be realized, then the recourse to pseudonyms will offer accordingly lower degrees of protection.

The possibility for observation and surveillance is not restricted to the content that a person is transferring over or making public on the Internet. At least as important is the information exposed when a user is surfing the Internet. In most cases the visited websites alone allow statements about the interests or the personal views and attitudes of the visitor. This picture can be refined by an analysis of the clicked links

and the time spent on different sub-pages. Inquiries at search engines provide for instance information about topics and problems currently occupying ones mind, about envisaged purchases or travels, or also about political views and sexual dispositions. New industries have emerged that are engaged in collecting these data and condensing them to informative personal profiles.

A specifically problematic aspect is the discrepancy and contradiction between the subjective impression of the user and the objective reality. Even when one is aware of the possibilities of observation, the private surfing of the Internet in front of a monitor in a separated space gives the impression of a higher degree of anonymity than for example quarrying in a public bookstore. However, one can be pretty sure that any step and any click in the cyber world is recorded and stored and that these data can normally be (re)-personalised – if no specific countermeasures are undertaken, whereas in the real world imperfect memories are wiping out all traces in a short time.

2.4 Pervasive Computing

As comprehensive and enlightening as the data that can be generated from the use of telecommunication services or of the Internet may be, they still leave large gaps from the perspective of perfect surveillance. On the one hand, they are bound to certain actions actively undertaken by the observed persons, be it merely the act of taking along a switched-on mobile phone. At least in theory one could evade surveillance by doing without telephone calls, Internet etc., although in modern society this would in practice often imply giving up full participation in economic and social life. On the other hand, all activities undertaken without using information or communication technologies are not covered.

With the diffusion of pervasive computing these gaps are likely to be closed step by step. An essential point in the vision of pervasive computing is the pervasion of everyday objects and surroundings with invisible information technologies that will assist people in all kinds of activities in an unobtrusive manner. The technology should be in the background, unnoticed by the users. Artificial interfaces such as keyboards – used today for entering commands – shall be replaced by a permanent observation and interpretation of the actions of the user, offering appropriate services or information when needed. Reality is still far from matching this vision; however, intense efforts are made to surmount open technical problems and to create the required prerequisites.

One of the basic technologies for pervasive computing is Radio Frequency Identification (RFID). This technology allows the assignment of unique identification tags to any object. The tags can be read automatically and unnoticeably from some distance. Biometrics can be used to identify an individual, but with extended capabilities this technology may allow interpretation of a person’s natural language, behaviour and emotional status.

Obviously permanent observation signifies a permanent threat to privacy. Ubiquitous information technologies also endanger privacy in less direct and apparent ways. They are in clear contradictions to the most important principles upon which current data protection. One of these principles is the purpose specification principle, which states that personal data may only be collected and processed for a purpose determined in advance. Pervasive information technologies can, however, fulfil their promises only if they are permitted to collect data without restrictions and evaluate them in permanent learning processes. A second central principle states that, with certain legally based exceptions, personal data may only be collected if that person's consent is given explicitly and voluntarily. In environments with ubiquitous computing it will be possible to be excluded because of a lack of consent (and payment) from the offered services, but not from the registration by invisible cameras and sensors. Technical progress in information technologies is at the same time increasingly endangering privacy and blunting the instruments for its protection; therefore new instruments, mechanisms and policies will be required to guarantee the survival of privacy in the future.

The apparent threats to privacy have induced large research activities to develop pervasive computing technologies and systems that respect privacy. However, so far these endeavours have had limited success; to achieve rather marginal gains in privacy one has to accept considerable restrictions in the usefulness, usability and user friendliness. It remains therefore an open question whether privacy friendly pervasive computing systems can be developed which still resemble the visions of pervasive computing. It is also still open which direction the development and implementation of pervasive computing will take and which concepts will prevail; whether more centralised concepts will be followed or more decentralised models based on wearable or portable technologies will be preferred. However, very simple, intermediary and personalised forms of pervasive computing like tiny electronic gadgets allowing lifetime video or audio recordings will cause dramatic changes as for any action or conversation could be captured at any time. The nature and the scale of the threats to privacy warrant increased research into future mechanisms for privacy protection and the initiation of broad public debates on the raised issues.

2.5 Privacy Enhancing Technologies

Technical progress does, of course, also offer new opportunities to protect one's privacy through technology. The cryptographic foundations for anonymous Internet use were developed already at the beginning of the eighties. These concepts were further improved and attempts undertaken to transform them into services and software once the Internet started to expand. In the middle of the nineties the term "PETs - Privacy Enhancing Technologies" was established for this field of technology (for more information on PETs, see 5.2.4). So far PETs have not fulfilled expectations that they would form an effective counterweight to the ever increasing surveillance potential. In theory they do offer sufficient protection, at least against unwanted

commercial data collectors. In practice, however, only users having extensive computer skills and willing to accept losses in convenience and in the range of usable services can benefit from these technologies. For an average user PETs do not prove useful and usable. In order to fulfil their potential PETs should be considered and applied as integral components of information systems and communication infrastructures instead of the currently prevailing form of end-of-pipe technology to be implemented by individual users. Specific measures and political backing would be required to build up privacy friendly, anonymity supporting infrastructures on a significant scale. The current dominance of security concerns in societal and political discussions makes such support quite unlikely. On the contrary, prohibitions and restrictions to existing services can be expected as they could obstruct the aspirations for a comprehensive surveillance and data retention scheme (see Chapter 3).

Whereas technology development embraces both new means to invade and to protect privacy, developments over the last decades strongly indicates that the privacy threatening potential is likely to prevail without specific support and concrete measures being taken. In the subsequent chapters many options for political guidance and intervention in key affected areas will be identified.

Chapter 3 Legislation – current situation and recent development

By Walter Peissl (ITA)

3.1 From Fundamental Right to Specific Regulations

There is a long tradition in European Constitution of safeguarding individual property, sanctity of the home and individual communication. These values were the origin of the broader basic right of privacy that was established later. It was first argued in 1890 by Warren and Brandeis, two lawyers in the United States, that new technologies (e.g. photography) establish new forms of intrusion and require the establishment of new rights for the individual. The right to privacy was defined as the "right to be let alone".[2]

The second half of the last century was characterised by several attempts to establish and guarantee the basic right of privacy by international agreements and national regulations. The basis was established with Article 12 of the Universal Declaration of Human Rights[3] and with Article 8 of the European Convention for Protection of Human Rights and Fundamental Freedoms in 1950.[4] The obvious danger that this human right could be threatened by the emerging electronic data processing was mitigated by specific regulations and agreements for this sector.

In 1960s and 70s there was a broad debate in several European states on the use of electronic data processing by public authorities that led to the initial national data-protection laws in the late 1970s. With Convention No. 108 from 1981 a treaty for the protection of human rights in relation to automated processing of personal data was passed.[5] The OECD developed a set of Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980.[6] Therewith the principal elements for the protection of privacy have been created. Those "Fair Information Principles" appear either explicitly or implicitly within all respective regulations.

---

[2] Warren, S. D., Brandeis, L. D. (1890): *The Right to Privacy*, Harvard Law Review IV(5), 193ff http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html

[3] UN (1948): *Universal Declaration of Human Rights, in: Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948,* http://www.un.org/Overview/rights.html.

[4] Council of Europe (2003): *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11 with Protocol Nos. 1, 4, 6, 7, 12 and 13*, http://www.echr.coe.int/Convention/webConvenENG.pdf

[5] Council of Europe (1981): *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[6] OECD (1980): *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980 http://www.oecd.org/document/20/0,2340,en_2649_33703_15589524_1_1_1_37409,00.html

Fair Information Principles:

Any organisation or authority…

- must be *accountable* for all the personal information in its possession
- should *identify the purposes* for which the information is processed at or before the time of collection
- should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances)
- should *limit the collection* of personal information to the amount necessary for pursuing the identified purposes
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (*the finality principle)*
- should *retain* information only as long as necessary
- should ensure that personal information is kept *accurate, complete and up-to-date*
- should protect personal information with appropriate *security safeguards*
- should be *open* about its policies and practices and maintain no secret information system
- should allow data subjects *access* to their personal information, with an ability to amend if it is inaccurate, incomplete or obsolete.[7]

These principles are, however, relative. Like other individual rights privacy must be balanced against correlative rights and obligations to the community, although the concept of "balance" and the process of "balancing" are highly ambiguous.[8]

3.1.1 EU-Directive 95/46/EC

One of the most important regulations at the European, and even at a global, level is the EU-Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This directive set standards for data protection and privacy policy within the European Union and far beyond. In its Art 1 the Directive states, that "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".

---

[7] Bennett, C. J. (2003): *Information Privacy and "Datenschutz": Global Assumptions and International Governance*, in: Peissl, W. (Ed.): *Privacy: ein Grundrecht mit Ablaufdatum? Interdisziplinäre Beiträge zur Grundrechtsdebatte*, Wien: Verlag der Österreichische Akademie der Wissenschaften, 61-81.

[8] Raab, C. D. (1999): *From Balancing to Steering: New Directions for Data Protection*, in: Bennett, C. J., Grant, R. (Eds): *Visions of Privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press, 68-93.

This directive was adopted because of the lack of progress towards practical implementation of the Fair Information Principles, and because private data processing was becoming more and more important within the European Union. As can be seen from the title of the Directive the aim was twofold: To “protect personal data” and to ensure “free movement of such data”. This shows that one of the objectives of the directive was to ensure an equal level of protection throughout Europe to facilitate free movement of personal data within Europe in order to establish the internal market.

The right to privacy prohibits any processing of personal data. To make data processing legitimate criteria were set out in Art 7 of the directive:

Legitimate data processing is only taking place if:

- the data subject has unambiguously given his consent; or
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary in order to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Additionally in Art.13 exemptions and restrictions were formulated. It is possible for Member states “to adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others."

Article 7 and Article 13 of the Directive show how the above-mentioned balance between privacy and other correlative rights and obligations to the community was conceptualised.

The Directive serves as a model with worldwide impact. The obligation to translate this directive into national laws within a fixed period of time should guarantee their practical effectiveness. The Directive is now implemented in almost all member states. To some extent these efforts have been successful, although there are still substantial differences in the enforcement and persecution of people and organisations that violate this Directive. The prohibition to transfer personal data to countries that do not possess an adequate level of privacy protection was putting pressure on Non-EU-Countries to adopt comparable regulations and so the EU-Directive became a model for privacy policy far beyond Europe.

3.1.2 Other regulations

Further pressure for adjustment originated from the technical developments described in Chapter 2. Due to the rapid technical progress of information and communication technologies and the resulting new ways of generating and analysing personal data the existing regulations were increasingly regarded as insufficient. This development induced the passing of new directives at the EU-level, e.g. the Directive 97/66/EC and 2002/58/EC[9] concerning the processing of personal data and the protection of privacy in the telecommunications sector and the processing of personal data and the protection of privacy in the electronic communications sector.

3.2 From a Prohibition to an Obligation

Protection of privacy was never perfect. On the contrary, in many cases large discrepancies between written law and daily practice existed, data protection authorities (established through Art. 28 of the Directive 95/46/EC) were lacking power and/or will to enforce regulations, and legislation lagged behind technical

[9] European Parliament and Council (1997): *Directive 97/66/EC of the European Parliament and of the Council of 15. December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*, Official Journal L 24/1 http://europa.eu.int/eur-lex/pri/de/oj/dat/1998/l_024/l_02419980130de00010008.pdf
and
European Parliament and Council (2002): *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)*, Official Journal L 201, 31/07/2002 P. 0037 - 0047.

developments. The protection of the human right of privacy was never regarded as an absolute right, but always seen in relation to and balanced with other fundamental rights, public requirements and economic necessities. Nevertheless a general consent existed; at least about the rough direction that development should take. Disputes concentrated more on the specifics of the implementation and the speed of the process.

The rules for data storage in the telecommunications and Internet sector looked as follows: Traffic data with personal reference were allowed to be stored as required for the delivery or billing of services. To be able to check possible queries regarding invoices, a storage period of about six months was regarded as reasonable. Content was not allowed to be stored at all, as long as the storage was not a part of the service itself – e.g. to deliver an SMS (Short Messaging Service) to a switched-off mobile phone at a later time. In these cases the content should be deleted as soon as no longer required. Law enforcement authorities were naturally excluded from these limitations if they could obtain a court order for surveillance.

Currently this balance seems to be under a lot of pressure. As a result of the attacks on New York, Madrid and London in 2001, 2004 and 2005 the societal security issue boomed. International policy now is to collect as much data as possible about potential terrorists by all means. In particular new ICTs provide a high potential for surveillance. Privacy is often given a lower priority than other societal objectives. There is little discussion on whether more surveillance really can contribute to ex-ante security and what the price is – in terms of loss of privacy and civil rights with corresponding negative impacts on personal freedom, democratic development and economic prosperity.

A key development in this area was the passing of the Cybercrime Convention of the Council of Europe in 2001. This agreement provides for extended authorisation of wiretapping Internet communications and of trans-border exchange of data. Internet communications shall be made open for real time interception, and provisions shall be made for the retention of traffic data. This convention came into force in mid 2004 and must be transferred into national law from this time on.

It is argued that the European Union’s new data protection Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, could lead to the undermining of an individual’s right to privacy. Article 15 of this directive contains a provision allowing the member states to enact regulations that cancel the prohibitions of data retention. On the basis of this opportunity some member states have launched initiatives to cancel the former prohibition of long-term retention of traffic data, and instead require such retention for periods between 12 and 36 months.

3.3 Concluding remarks

We now face a situation where different fundamental objectives are conflicting. Even basic rights are not unchanging and have to be adapted to emerging societal needs. But it is necessary to balance arguments very carefully. It was first the economic value of personal data in a global market that put increasing pressure on the protection of privacy. Nowadays it is people's fear in times of uncertainty that lead too often to simple solutions like "more surveillance equals more security".

Both these arguments lead to weakened privacy. Some say that this trend constitutes a long-term danger for democratic and even for economic development. In the following chapters we will discuss different trade-offs in more depth and suggest ways a balance might be struck between different fundamental rights and societal objectives.

Chapter 4 Security

By Chandrika Nath (POST) and Walter Peissl (ITA)

4.1 Issue at stake

ICT applications can be used to enhance societal security. The events of September 11th 2001 highlighted existing concerns over the vulnerability of modern society to terrorist attack and led to increased efforts to strengthen security arrangements at national and EU level. These efforts have led to increased surveillance of citizens, giving rise to concerns that the internationally acknowledged fundamental right of privacy is being jeopardised. The longstanding debate over the value of societal security versus individual freedom is growing increasingly polarised; there is a widespread perception that there must be a "trade-off" between security and surveillance. In this chapter we address the validity of this perception and ask the question "does surveillance really lead to more security? And if so, how great a price will citizens have to pay for this increased security?"

The term "Big Mother Society" has been coined to describe a scenario where a large number of independent decisions are taken to enhance security for the collective benefit of society. While each independent decision may not be a serious threat to individual privacy, some commentators argue that the overall effect can be comparable to the more frequently cited "Big Brother" scenario.

In this chapter we discuss the impact of some applications that aim to increase collective security, such as CCTV for crime reduction.[10] We discuss the extent to which some current applications adhere to the principles of proportionality, relevance and functionality outlined in earlier chapters. Drawing mainly on projects carried out by EPTA partners we discuss the opinions of both lay people and experts. Section 4.2 discusses technologies, section 4.3 discusses social and economic factors, and section 4.4 describes political and legislative factors.

4.2 Technological developments

There are two ways to enhance security in systems. The first is to restrict entrance to the system to authorised people only. The second is to monitor and survey the system. Thus security related applications may be arranged along two main criteria: technologies for identification and authentication, (such as biometrics, ID-cards, digital imaging, iris scanning); and technologies for surveillance. Security technologies range

[10] We do not address the potential for such technologies to increase individual safety (e.g. locating individuals in an emergency using location based technologies).

from relatively well-established technologies such as Closed Circuit Television (CCTV), to those which are only just emerging, such as pervasive computing. In all cases the issues raised are similar: are people aware that they are being watched? How secure is the personal data? How long can it be stored for? Who has the authority to access it? Does it really enhance security or is it just a perceived benefit? Below we discuss some specific technological developments, which have formed the focus of recent EPTA projects and the issues arising from them.

4.2.1 ID cards and biometrics

Identity cards are not new phenomena – they have been used across Europe for many decades. Most EU member states have implemented a form of ID card. The only members currently without any form of identity card scheme are the United Kingdom, Ireland, Denmark, Latvia and Lithuania.[11] Renewed debate over ID cards is arising because of advances in ICT. Firstly, ID cards can now be used in conjunction with digitized information (for example biometrics or digital signatures). These provide the ability to uniquely identify an individual, and thus could be used, for example, to prevent fraud, control immigration and combat crime as well as for non-security applications – e.g. access to public and private sector services.

Belgium was the first country in Europe to introduce such digital cards – a digital signature has now been embedded into all ID cards in Belgium, which allows citizens to perform more secure transactions, for example with government. Similar systems are being considered by a number of other countries. The Austrian social-security card (e-Card) is capable of holding additional information which will allow it to be used as a “Bürgerkarte” in future e-government applications. There has been heated debate in the UK over government plans for ID cards. Under current UK government plans, ID cards would be used in conjunction with a biometric identifier, which would allow access to over fifty different types of data on an individual, stored on a centralized database. This controversial scheme has been described as the most comprehensive card system proposed in Europe to date.

The kind of identifier used, transparency over the stated purpose of the ID card scheme, the kinds of service that can be accessed, and how the data is stored (i.e. whether on a localized or a centralized database) are all key factors determining public acceptance of ID card schemes, as EPTA studies show. This also holds for the new European passport, which will have incorporated biometrics like digital images as well as electronic fingerprints (Biometric passports [NBT 2005]).

[11] Fourth report of the House of Commons, Home affairs Select Committee session 2003-2004, July 2004.

4.2.2 CCTV

Closed circuit television surveillance of public areas is widespread across Europe. The UK has been described as “the most surveyed population in the world”; it is estimated that the average Londoner is captured on camera over 300 times a day! Guidelines vary in different countries – but even when, as in the UK, they stipulate that cameras in public places should be clearly marked, this particular specification is not always followed. As systems become more sophisticated, covert use is becoming easier. Wireless cameras can now even be built into household devices with the same convenience as alarm clocks or vacuum cleaners. So people are not always aware they are under surveillance.

While the earlier CCTV systems were analogue, digital systems are becoming increasingly widespread, raising new privacy concerns. Digital image searching can save time in the locating of specific events or tracking crime suspects against an existing database.[12] However, in 1998 the Science and Technology Committee of the House of Lords noted the potential ease with which digital images could be copied or manipulated, even on a home computer system.[13] Although authenticity can be established using audit trails or watermarks, the potential for image manipulation is still a concern. The privacy implications of “Intelligent CCTV” are an emerging area of debate. Their use is being investigated by many authorities – automated recognition technologies could track “suspicious behaviour” or spot suspicious packages.[14]

4.2.3 Electronic surveillance

In principle “electronic surveillance” refers to all forms of surveillance of digitised data, including digitised CCTV images that have already been discussed. It also includes surveillance of traffic or communications data (or increasingly location data) from the internet or mobile phones, or data generated by the use of shop cards, credit cards or ID cards. The existence of large databases opens up the possibility of data mining. This may be used for commercial activities (discussed in more detail in Chapter 8) but could be used also to spot patterns of activities which can be classified as “suspicious”. In recent years there has been a trend towards increased electronic surveillance by governments at the expense of individual privacy. “Anti-terror” legislative packages have been introduced in many countries across the world over the past few years. For example in the UK the controversial Regulation of Investigatory Powers act, introduced in 2000, was intended to provide public authorities with new powers to fight terrorism and crime, including powers to intercept

---

[12]West Yorkshire Police, Imaging unit: *Video and CCTV*: http://www.westyorkshire.police.uk/section-item.asp?sid=6&iid=111

[13]Fifth report of the House of Lords, Science and Technology Select Committee, February 1998.

[14]Tendler, Stewart (2005): *'Smart' CCTV could fight terrorist threat in stations*. Times online http://www.timesonline.co.uk/article/0,,2-1872083,00.html

or access details of electronic communications and to demand plain text of encrypted messages. However just as authorities develop new surveillance techniques, criminals can use the same or derived technologies to avoid being traced – for example by "spoofing" (sending out false messages or covering-up the exact address of the sender of a message) to misdirect authorities or by encrypting data and communication (as sophisticated encryption technologies are publicly available). The most prominent and widespread system of electronic surveillance is the ECHELON network (see text box).

Echelon

The Echelon network is run by an alliance between the USA, UK, Canada, Australia and New Zealand. The system has been in operation since the cold war. It was initially set up to monitor communication in or to the Soviet Union and Eastern Europe. The existence of the system was widely publicised as a result of a report from STOA (Scientific Technology Options Assessment).[15] As the alliance itself refused to comment, the EU Parliament appointed a committee to consider the existence of Echelon and its methods. The committee concluded[16] that the system exists, and that its purpose is to monitor private and non-military communication. It is stated that the system can perform quasi-total surveillance, which means that all types of electronic communication – telephone conversations, SMS, fax, e-mail and internet traffic – can be monitored. Patterns of communication can be analysed, and content can be scanned for interesting keywords. Messages that are identified by the system are copied for manual evaluation. The EU Parliamentary Committee advised both business and individuals to apply measures to avoid surveillance. A report by the Norwegian Board of Technology recommends that Encryption of communication should be the norm, rather than the exception (Echelon [NBT 2005]).

At present individuals can avoid surveillance and maintain some degree of anonymity simply by not using telephones or the internet. However, if pervasive computing becomes a reality, surveillance could occur without their knowledge or consent, and current principles of data protection would be rendered obsolete. Although such scenarios remain some years into the future, the technologies involved are developing rapidly. One example is RFID tags, which are seen as the next generation of 'bar codes' (a common form of optical identification). However, unlike bar codes, which can only be used to identify a *type* of product, RFID tags can store a large amount of information and can therefore be used to uniquely identify a product ("item level

[15] Steve Wright: *An appraisal of the Technologies of Political Control*, Omega Foundation, European Parliament (STOA), 6 January 1998; Duncan Campbell: *Interception Capabilities 2000*, IPTV Ltd, European Parliament (STOA), 1999.

[16] Temporary Committee on the ECHELON Interception System: *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system),* European Parliament, 11th July 2001

tagging") or to store personal data. Previously tags were only used in closed systems – e.g. within the supply chain of individual retail companies. However they may be used for security applications. RFID tags have been shown to reduce laptop theft in UK trials. They can also be used in different forms to track individuals: there are discussions about RFID tags being used to track the homeless, criminals and children.

4.2.4 Technological limitations

The security of digitised data, particularly the security of large databases, will be of key importance as far as public confidence is concerned. Although there may be strict rules on who can access such data, any access by unauthorised individuals as a result of security breaches could have serious consequences for privacy which could seriously undermine public confidence. The UK tabloid newspaper the SUN claimed in 2005 that it had purchased personal details of banking customers (including addresses, passport data and passwords) from a Delhi IT worker for just over £4. Public trust, once lost, is unlikely to be re-established easily. Breaches of security are of particular concern in cases where more information is stored than is necessary for a given application. For example biometric data may contain information on ethnic origin that would be irrelevant to most applications and could be misused if the data fell into the wrong hands (Electronic Traces [NBT 2005]).

In many cases there are concerns that the use of ICT, while impacting on privacy, does not result in any real increase in security. A report by crime reduction charity NACRO in 2002 questioned the effectiveness of CCTV, claiming it only reduces crime by 5% (compared to street lighting which was found to reduce crime by 20%). The UK Home Office (HO) has since carried out a review of existing research. While this review pointed to a number of case studies where the use of CCTV has resulted in reduced crime – for example studies show a 41% overall decrease in vehicle crime in car parks where CCTV has been installed - it concludes that "*further high quality research is needed into CCTV to find out more about how CCTV works and where it works best*". The HO argues that CCTV works best as part of a package of measures to reduce crime. The URBANEYE Report points out many limitations in the available research on the effectiveness of CCTV, and argues that many reports "*highlight statistics in order to justify the effectiveness of CCTV*"[17]

These technologies may themselves give rise to new forms of crime – for example identity theft that is becoming an increasing problem in many countries. A UK survey recently commissioned by the software firm Intervoice found that concerns about

[17] http://www.urbaneye.net

identity theft were beginning to deter people from internet shopping and banking – 17% said they had stopped web shopping and 13% had stopped banking online.[18]

4.3 Social/cultural developments

4.3.1 Attitudes to surveillance

Attitudes towards ICTs, and to the loss of privacy associated with them, depend on the intended application. For example in the Danish investigation of attitudes to citizens cards, it emerged that while citizens were happy to use such a card to provide them with access to various public or private services, there was opposition to the idea of an ID card that had to be carried at all times. Similar opposition to ID cards has been encountered in the UK. In the case of electronic surveillance, citizens in the Danish discussions (Citizens' card [DBT 1994]) made the distinction between "Big Brother" style surveillance, and "friendly control" where technical improvements in systems used to keep track of taxes, etc, and are used to uncover fraud. While there was opposition to the first scenario, "friendly control" was regarded more favourably. Citizens felt that "friendly control" would reduce the need for citizens to report each other for fraud, a task they saw as the responsibility of the government. Citizens in the Danish studies made it clear that they wanted to be well informed about their rights, and protected against too much unnecessary surveillance.

The need to allow some private space to individuals was also raised. For example while mobile technologies can increase safety by allowing people to be located in emergencies, participants were concerned that their excessive use did not leave enough private space for individuals. Participants felt that children should be allowed to have some private space. They raised concerns over the fact that parents can now put up web cameras ("webcams") in nursery schools (Electronic surveillance [DBT 2000]). The citizens in the Danish study saw parental surveillance as fulfilling a need for control on the part of adults – not a need of the children. The lay panel feared this could lead to the children only acting in a way they assumed their parents would approve of. Also in the Danish studies citizens made it clear that they did not want surveillance to replace the sense of social responsibility and caring for other people (Electronic surveillance [DBT 2000]).

4.3.2 Trust in authorities

Attitudes to increased state surveillance depend on the level of trust placed in those authorised to view any data collected. There are cultural variations in the level of trust placed in "authorities". In the Norwegian focus group study participants showed great confidence in the government and large corporations, like Telenor (Norway's biggest

[18] BBC News (2005): *Public worried by online ID theft,* http://news.bbc.co.uk/1/hi/technology/4575255.stm

telecom company), to handle their data properly (Attitudes to privacy [NBT 2004]). When confronted with the dilemma of increased surveillance versus security/crime fighting issues, most felt that it was more important to fight crime than to uphold the right to privacy. They did, however, stress that only authorised personnel should have access to the information. On the other hand, citizens in the Danish studies were more sceptical of "Big Brother" scenarios, as mentioned previously, although they could see some advantages to surveillance.

4.3.3 Who is accessing the data?

Although the main threat is generally seen as coming from unauthorised access to personal data, in practice those "authorised" to access data can also abuse this authority. This is well illustrated by a recent case reported by BBC news where four UK council workers were charged with misconduct and attempted voyeurism for having deliberately pointed a street camera into a woman's flat. In another instance images of a man trying to end his own life were released by Brentford Borough Council to the BBC.

4.3.4 Function creep and data sharing

There is also the risk of "function creep" - data collected for one purpose being used for other undeclared or unauthorized purposes. A report by the Norwegian Board of Technology cites suggestions to open the central database of biometric identifiers of passport holders to other (commercial) actors. They would then be allowed to produce identity cards and to verify identity against the central passport database in exchange for a fee.[19] It has also been postulated that biometric information obtained as a result of tracking passengers for airline security purposes, could in principle be retained and used to collate information on passengers' movements and identify passengers of general interest to the authorities. This could lead to a risk of discrimination. For example, a retina scan at an airport might reveal an individual is susceptible to stroke. The information could be released without the individual's consent and lead to discrimination by employers, insurers, etc.[20] Fear of such scenarios could make passengers unwilling to voluntarily offer biometric scans. In the case of biometrics, the human rights group "Liberty" suggests that where biometrics are used and seen to be used for a clearly defined and stated purpose, the technology will be more acceptable to the general public.[21]

The URBAN EYE report points out that CCTV systems deployed for traffic management purposes in major German cities have been used for the observation of

[19] Biometric Passports [NBT 2005]
[20] Biometrics [POST 2002]
[21] Biometrics [POST 2002]

"social fringe groups". Another issue is the increasing amount of biometric data shared between governments through international databases. Concerns have been raised by human rights groups such as Liberty). Questions arise such as "under what conditions it is acceptable to share data on certain individuals", and "how such groups (e.g. suspected terrorists) can be defined?"

4.4 Legislative/policy developments

The increased emphasis on national security and counter terrorism in recent years is reflected in European legislation such as the EU's new data protection directive,[22] under which it becomes an obligation to retain traffic data (such as communication traffic) for between 6 and 24 months. Previously holders of such data were obliged to delete the data after the expiry of a specified period (usually a few months).

As pointed out in a paper by ITA[23], "anti-terror" legislation packages implemented in many countries following September 11th 2001 had implications for electronic privacy. One example is the UK's Anti Terrorism Crime and Security Act 2001, which led to new powers being granted to authorities to access traffic and communications data (the Regulation of Investigatory Powers Act 2001). The ITA report also points out that the range of tasks that could be accomplished anonymously on the Internet was much reduced, limiting the potential scope of privacy enhancing technologies.[23]

Even where regulation does set out to protect privacy, it is logistically difficult to enforce. [POST 2002] on CCTV points out the difficulties involved in enforcing regulations on CCTV usage (for example the requirement that cameras should be clearly signposted). This POSTnote stated that in the UK enforcement is reactive, as it is always in response to complaints. It is not clear whether legislation can keep up with the rapid pace of technological development, as discussed earlier in the context of the development of pervasive computing. In the Danish Consensus Conference on Electronic Survey (Electronic surveillance [DBT 2000]) both citizens and experts agreed that the constantly changing picture of surveillance demands ongoing debate and adjustment of legislation. In Denmark the Act of processing Personal Data (act no. 429 of May 2000) is not adequate to meet the challenges of applications such as e-government. The Danish Data Protection Agency, the body that monitors the act, has experienced cutbacks during the last 2-3 years. This concerned some of the juridical experts that took part in the consensus conference.

[22] Directive 2002/58/EC
[23] Peissl, W. (2003): *Surveillance and Security – a dodgy relationship*, Journal of Contingencies and Crisis Management 11 (Number 1), 19-24.

4.5 Concluding remarks

The use of surveillance technologies is increasing due in part to the rapid implementation of anti-terror legislation over the past few years. With the digitalization of ICTs such as CCTV, and the presence of a number of surveillance technologies throughout cyberspace, the potential for surveillance of citizens has increased. A key question is whether the implemented technologies actually increase security or whether they are simply perceived as enhancing security. Do the technologies enable the police to identify criminals, or do they simply increase the number of (innocent) suspects[24]? Do the technologies have a clearly stated purpose at all? As well as concerns over the risk of inappropriate use of public money, concerns are raised over the long-term societal impact of surveillance. There is only a limited understanding of the psychological impact of surveillance and more research should be conducted in this field.

[24] Schneier, Bruce (2005): *Beyond Fear. Thinking sensibly about security in an uncertain world*, Copernicus books.

Chapter 5 Access

By Johann Cas (ITA) and Christine Hafskjold (NBT)

5.1 Issues at stake

Access to ICTs is of ever increasing importance for full participation in economic and social life. Provision of private and public services is more and more based on ICTs, e.g. in numerous e-Commerce or e-Government applications. How can users get access to these in a secure and privacy-friendly way? Another privacy issue concerns access to existing data, where there are many different issues to consider:

- How to secure these data and impede unauthorised access?
- How can we increase transparency and to provide access to personal data, allowing the user to correct or update his or her own data if necessary?
- How should the question of consent be handled? When is consent from the data subject needed? How can a previously given permission to store and use personal data be withdrawn?

As a result of the rapid development in modern ICT we leave electronic traces almost whatever we do and wherever we go. This leads to an enormous quantity of data, which can be tempting to use or abuse. The fact that such data pools exist may also encourage new regulations further limiting the few possibilities of anonymous or pseudonymous use of ICT services that are available today. To ensure confidentiality, it is important that personal information is stored in a secure way, and that access to the information is for authorized personnel only. The access should also be logged, so abuse of trust can be detected at a later stage.

More and more European governments aim to make their public information and services available to their citizens online. For services involving personal information, the user will need some form of secure log-on mechanism, like a citizens' card or a digital signature. However, a general threat with this type of technology is that it encourages extensive requirements for strong identification even for non-critical transactions.

Another issue at stake concerns a data subject's access to personal data, and the restrictions necessary to protect the same data from unauthorised access. Access to personal data is needed to fulfil data protection regulations requesting transparency of data collections and opportunities for the data subjects to correct or delete their personal data. In Denmark, an expert group working for the Danish Board of Technology recommends that the right to view and correct personal data should be extended: The user should also be able to see the entire course of his or her case, and to control who else has viewed and/or changed their data (from the logs).

The right to access personal data is already difficult to exercise and seldom requested. For future pervasive or ubiquitous computing environments even the principles to guarantee this right are unknown.

Access to services means inclusion and participation; denial of access or the need to give up privacy for getting access can cause new forms of social exclusion and of digital divide, adding to a digital divide caused by lack of knowledge or of financial resources to make use of new media and services. New potential causes of this "privacy divide" can be a lack of technical skills required for using privacy enhancing technologies (PETs) or a resistance against sacrificing personal privacy.

5.2 Technological developments

In this section technological developments of particular interest for access and inclusion beyond the general tendencies are addressed.

5.2.1 Electronic identification

Citizen cards or other forms of Public Key Infrastructure (PKI), including the digital signature they may contain, are increasingly promoted as a means of (secure) access to e-government services. For specific application areas they are offering clear advantages, e.g. more secure access to critical services. They may also be more convenient than using several different password and/or PIN combinations.

In general, the demand for digital signatures from individuals is low. The few and infrequent contacts with public administration requiring identification hardly justify the need for digital signatures for normal citizens. The same holds for commercial transactions; only a few require any identification at all, and those which do are usually conducted with the assistance of a notary or another authorised person, e.g. real estate business.

The introduction of electronic identification/digital signatures is not necessarily privacy threatening if applied in a privacy aware and enhancing manner. It can even increase privacy if it is used to introduce PETs in e-government. An attempt to do so has been undertaken in Austria, though with conflicting evaluation by different parties. The developers and the Austrian Data Protection Officer state that the concept has a strong data protection orientation, but the need to identify at every point of contact is criticized by privacy organisations. It is a general concern when a strong form of identification is introduced, that it becomes much easier to require the user to authenticate himself at a much earlier stage than necessary.

This tendency may also extend to private services or e-commerce in general, specifically if public and private functions are merged on a single card. Multifunctional cards can accelerate deployment and may also be more convenient to the users, but they involve additional privacy and trust issues. The use of e-commerce services

regularly requires identification, at least for payment, whereas in day to day offline shopping hardly anyone would accept the request of identification before settling a transaction. Models for both secure anonymous electronic payments and for using trusted third parties for physical delivery exist, but they have so far not been successful on the market.

5.2.2 RFID (Radio Frequency Identification)

RFID is a technology with enormous potential privacy impacts as it allows the allocation of unique identification codes to virtually any object, animal or person. Concerning access the range of applications reaches from incorporation of RFID tags into personal documents like passports or identity cards to the replacement of traditional means of obtaining permission to use certain services, for example public transport, sport facilities or cultural events. These applications are highly relevant for access to specific services as well as for participation in public life at all as many countries require from their citizens to carry permanently personal identification documents with them when moving around in public space.

The two main dimensions threatening privacy are the possibility of remote and undetected reading of the RFID tags on the one hand and uniqueness of the tag with subsequent possibilities of personalisation on the other hand. The extent to which these threats may be realised can be limited by technical design of the systems deployed, e.g. metallic shielding of RFID equipped documents against unnoticed remote reading, or encryption as protection against unauthorised reading; such measures need to be incorporated into systems design from the beginning.

5.2.3 DRM (Digital Rights Management)

DRM technologies regulate or restrict access to digital content. Their aim is to enforce copyrights that can be very easily overcome in the digital world where information can be copied and transferred without losses in quality and at a very low cost. DRM technologies are disputed for several reasons, for example will they promote or hinder the further development of the information society? What long term impacts the introduction of artificial barriers to the flow of information have? An important aim of DRM technologies is to offer far more possibilities than a simple protection against copying: With DRM it is possible to control the number of uses, the quality of presentation, the kind of devices that can be used for access, the number of copies that can be made and so forth. This means that the price can be differentiated based on the level of service the user wants.

The impacts on privacy will to a large extent depend on the particular design of the DRM systems deployed. Systems that require the customers to identify themselves to get access to the content are endangering personal privacy, as their tastes, preferences and habits are being exposed (DRM [NBT 2005]).

5.2.4 Privacy Enhancing Technologies (PETs)

PETs can be applied to mitigate or eliminate the trade-offs between getting ICT assisted access to services and preserving privacy. One use can be to separate the data used for authorisation (i.e. to establish that a person has the right to access the service) from the data used for personal identification. An important function in this respect could be to provide for anonymous electronic payment. Attempts to introduce such schemes have so far not been commercially successful. The implementation of the principles of data minimisation by technology could also apply to Identity Management (IM). IM is expected to grow in importance as the multitude of verification, authorisation and identification processes make technical assistance in the management of different user name and password combinations (digital identities) a beneficial and lucrative task.

So far PETs have not contributed as much as would be possible to the protection of privacy; partly because of a lack of availability of PETs, partly because of a lack of user friendliness. The many difficulties that a privacy aware user has to face –from minor inconveniences to a total loss of access to certain services – and the know how required to make use of many PETs, can to some extent also explain the often observed discrepancy between stated concerns about privacy and actual behaviour. On the other hand PETs could play an important role in making use of and access via ICTs more secure and convenient. A growing security issue today is identity theft, a problem that would diminish if access was not bound to identification, but to secure digital credentials.

5.3 Social and economic developments

Digital divides exist on different levels: They divide the rich from the poor, the skilled from the inexperienced and, on a global scale, the north from the south. Privacy, or the desire to preserve it, may establish a new division, a privacy divide, which reinforces existing barriers. The need to spend money to use new access technologies or to invest time in learning to use creates a trade-off between access and privacy.

As stated previously, most PETs add a complexity to the technology they are designed for. Whereas the recommendation to make use of PETs in principal can protect the privacy of an individual considerably, the practical deployment of these technologies often requires advanced know-how. In addition, the user often experiences reduced accessibility of service, poorer performance, additional costs for software and services. Appeals to individual responsibility, either to use PETs or to do without privacy intrusive services, are more and more difficult to follow as full participation in economic and social life is increasingly depending on the use of ICT.

5.4 Political and legislative developments

Concerning access, the role of PETs as a potential means of providing privacy protected access is used to exemplify political and legislative developments. Whereas the technical problems of privacy enhancing technologies are largely solved, political and legal support for widespread use is largely missing. The current trends in legislation (see Chapter 3) make stronger support of PETs rather unlikely: The introduction of obligations to provide anonymous access to services or infrastructures would directly contradict the strong endeavours for mandatory retention of telecommunications and Internet traffic data. A significant privacy-divide between average users and those willing and capable of protecting their privacy will probably be the consequence.

5.5 Concluding remarks

ICT supported access is becoming increasingly important for a wide range of public and private services. For technical and economic reasons, and as a result of political trends, privacy is under increased pressure. In addition to a digital divide, a privacy divide could become more apparent in the future. This may take different forms:

- As more and more services demand that the user identifies to gain access, privacy concerned persons could be excluded from full access to services vital for social, economic and political inclusion and participation.
- The availability and awareness of PETs has been limited. If left to individual citizens alone we might see a “privacy divide” in the future, between those who are aware and have the skills needed to protect their privacy, and those who do not. The latter may be vulnerable to the exploitation of their personal data.

To avoid a privacy divide, it is important that privacy concerns are addressed at the design stage of new projects. All projects that involve personally identifiable information should include a Privacy Impact Assessment. Consideration should always be given to the feasibility of integrating privacy enhancing features such as anonymity and pseudonymity into the system.

Chapter 6 Societal interaction

By Rinie van Est (Rathenau), Christine Hafskjold (NBT) and Janus Sandsgaard (DBT)

6.1 Issue at stake

Within the last decade, Internet, webcams, e-mail, smart cards and mobile phones have become commonplace technologies. Social use of ICT is an important driver for the development of ICT. In turn, these technologies have changed the way social interactions are organised, people construct their identity, shape their lives, and participate in social networks. Think only about new phenomena, like MSN, on-line sex, “Nannycams” etc. One third of all Dutch teenagers regularly visit the interactive gaming website Habbo Hotel, a virtual Hotel where they can chat and date, create their own personal space, and take part in a variety of competitions.

Although the acceptance rate of new media is very high among the digital generation, there exists little scientific knowledge and societal reflection about the nature and impact of this emerging integration between ICT, social interaction and privacy.

6.1.1 Social interaction and privacy

In Western democratic societies, privacy is the concept that embodies individual freedom. Individuals are free to be and become what they choose, free to be different, free to determine behaviour, free to choose a social personality, free to interact with others, free to choose a path in life, and so on.[25] The value of privacy for both the individual and society is immense. Privacy is valuable for developing our unique interests, personalities and social relationships in a way that is not always compatible with social norms. Accordingly, privacy is indispensable in a community that recognises social freedom as a good.

The value of privacy is never absolute, however. The human need for social interaction implies revealing some personal, often private, information, and thus losing some privacy. Accordingly, total privacy – a *No Brother* scenario - is not a real option for a human being. The boundaries of privacy depend upon the type of social interaction and the kind of information revealed. For example, in intimate and trusted relationships people are often less careful about certain things they say and do. With complete strangers concerns about privacy are also less significant, since in such a situation in a sense we are anonymous.

[25] Gutwirth, Serge (2002): *Privacy and the information age.* Lanham: Rowman & Littlefield.

In the debate about ICT and privacy Orwell's *Big Brother* scenario (total loss of personal privacy) plays a central role as an image of the future, which has to be avoided. But it's important to bear in mind that ICT not only presents a threat to privacy, but ICT can also strengthen privacy. For example, the internet, by enabling that many of our activities can be carried out within the privacy of our home, can increase the degree of our privacy.[26]

The same technologies that may increase privacy have made it possible to invade this privacy by monitoring and recording our behaviour. An example might be firms that use software which monitor internet use of employees, or similarly parents monitoring children. To prevent such privacy invasion, new social strategies and (related) privacy enhancing technologies (PETs) are constantly being developed. To deploy such strategies the one being watched has to be aware of the fact that he is being monitored. However, whereas in the past it was our neighbours and associates who invaded our privacy, now it is faceless strangers who may do so.

In summary, the relationship between social interaction, privacy and ICT is highly complex. First, privacy is a context-dependent property and social beings willingly compromise their privacy with their wish to maintain significant personal and social relationships. Second, besides invading our privacy, ICTs may increase privacy. Third, ICTs may change social interaction and even our sense of privacy.

In this chapter, we will describe the technological, social and economic developments that may relate to the issue of social interaction and privacy. In the final paragraph (section **Feil! Fant ikke referansekilden.**) some conclusions are drawn.

6.2 Electronic traces and profiling

ICTs have become an integral part of the social fabric. As a result more and more social interactions are mediated by ICT. This digitisation of social interactions results in a whole range of electronic traces. When you use your mobile phone, you leave a record of when you made the call, who you called, how long you were on the phone, and where you roughly were when you called. People leave digital footprints when surfing the Internet, borrowing a book from the public library, buying something in a shop by using a credit card, et cetera. In many cases the users are not aware of the many traces they leave through the use of ICTs. The use of various technologies can lead to different types of electronic traces that together might give information about a person's behaviour or social life.

[26] Ben-Ze'ev, Aaron (2004): *Love online. Emotions on the Internet*. Cambridge: Cambridge University Press.

The use of mobile phones, including new location services such as *FriendFinder©* which allows specific users to be informed about each others location, cars with GPS and automatic toll booths, video cameras that spot you while moving through public space all result in traces that might be used to put together mobility or communication profiles. Internet users may leave traces that can disclose personal interests, political attitudes or sexual predispositions, as they may be unaware of Spyware on their computers. (Data Prevention [ITA 02])

Personal web logs are becoming increasingly popular as a medium for publishing personal reflections on everyday-life, politics, terrorism or whatever the person feels like communicating. Both web logs and personal websites will appear on search engines. Employers who want to check persons applying for job can use this personal information. Being on the web with its global distribution, and the fact that search engines store information that has been taken off the web logs, also means a huge surveillance potential.

New and/or cheaper electronic technologies have enabled an increase in surveillance of the social behaviour of citizens in public and private spaces. In order to scan for theft or other criminal activities video cameras (CCTV) and webcams are installed and used in more and more places, for example in shops, schools, busses, on streets or at work. (Electronic Surveillance [DBT 00]) Digital convergence leads to new kinds of privacy threats. For example, people taking each others' pictures with mobile phones and publishing these on the internet, often with a person's name. (Electronic Traces [NBT 05]) These traces can be stored and might confront the traced person at inconvenient or unwanted moments. For example, in Flanders a teenager put a (private) nude photo of his former girlfriend on the web after she had broken up their relationship, and similar examples can be found around Europe.

In addition to the increase in the amount of traces, the traces contain more comprehensive information about the users and their actions. (Electronic Traces [NBT 05]) Electronic networks enable exchanging and combining of data. New methods of data analysis and data mining are arising from the increased quantity and quality of data gathered by the increasing use of ICTs. (Privacy in Austria [ITA 00]) In the early 1990's, private companies started collecting huge amounts (billions) of records, primarily for marketing purposes and to make services more efficient and convenient for users.

The strong growth of the number of digital footprints is likely to continue into the future, in particular if visions of the information society, such as pervasive computing, as promoted by industry, are to be realised. The idea of ubiquitous computing environments seems to be in contradiction with principles of privacy protection, such as collection limitation or purpose specification. Existing regulation may become obsolete before new methods of privacy protection are being established (Ubiquitous Computing [ITA 03]).

6.3 Social and economic developments

Full participation in social life increasingly depends on the use of ICTs. In 2005 almost all Dutch teenagers use the Internet and mobile phones. We are moving towards a real time of dependency, where if we lose our mobile or the computer server is down, we begin to feel cut off from our network of friends and colleagues.

6.3.1 Experience economy

Various authors have reflected on ICT's role in shaping personal lives and culture. For example, Pine and Gilmore (1999)[27] describe the metamorphosis from industrial production to cultural capitalism or the so-called experience economy. ICT plays central stage in this shift. Castells (1996: 373) captures the impact that the digital revolution is having on culture

> *"All messages of all kinds become enclosed in the medium, because the medium has become so comprehensive, so diversified, so malleable, that it absorbs in the same multi-media text the whole of human experience, past, present, and future."*[28]

In his book *The Age of Access* Rifkin (2000) critically assesses the commodification of human culture and the fact that more and more daily interactions with our fellow human beings get bound up in commercial relationships. Rifkin argues that

> *"By controlling the information and telecommunications technologies by which more and more people communicate with one another, marketers come to play the role that schools, churches, fraternal organisations, and neighbourhood and civic institutions used to in interpreting, reproducing, and creating cultural expression and maintaining cultural categories."*[29]

6.3.2 The Digital Generation

A the Rathenau Institute's workshop on *The Digital Generation* (March 17, 2005)[30] – young people born after 1980, which form the first generation that have grown up with internet, e-mail, and computer games - led to the following conclusion that seems to fit Rifkin's analysis:

---

[27] Pine, B. Joseph II, and James Gilmore (1999): *The experience economy: Work is theatre and every business a stage*. Cambridge, MA: Harvard Business School Press,

[28] Castells, Manuel (2003): *The rise of the network society. The information age: economy, society and culture*. vol. 1 Cambridge, MA: Blackwell

[29] Rifkin, Jeremy (2000): *The Age of Access: How the shift of ownership to access is transforming modern life*. London: Penguin

[30] Van 't Hoff, C., Q.C. van Est en A. Krom (2005): *De digitale generatie. Een blik op de toekomst van de informatiesamenleving via de generatie die als eerste is opgegroeid met ICT*. Den Haag: Rathenau Instituut, Sociaal Cultureel Planbureau

> *"ICT empowers young people to shape their lives more independent from their parents and teachers, who have little understanding of what these youngsters are doing in their virtual world. Traditional educators are more and more being replaced by peers, companies and other on line contacts."*

The gaming website Habbo Hotel[31] is an example of a commercial virtual space that is controlled by all kinds of 'zero tolerance' social rules. Parts of conversations are being stored and can be used as evidence for banning people from the website, and obscenities are automatically replaced by the word 'bobba'.

Commercial firms use interactive gaming websites for binding (young) customers into branded communities. Young people visiting the website are sceptical to giving personal information when prompted for it, but are generally willing to give it away if they are offered something in return (e.g. content, games or free SMS/MMS messages). The firms can use that information for marketing purposes. Regularly aggressive marketing that breaks privacy rules is used.

6.3.3 Low privacy awareness

Until now, the widespread social use of ICTs seems not to create great concern about the erosion of personal privacy. The Norwegian focus group study for example revealed that very few people both in the age group bands 17-19 and 30-40, had any knowledge about what kind of traces they leave behind when they surf the internet or use their mobile phone. Almost no-one knew about cookies, and even fewer deleted them. Within this group, young people did not feel their privacy was invaded when images of them, taken using mobile phones, were placed on the internet. "The general opinion was that if you wanted to avoid it, you should take the appropriate measures yourself." (Attitudes to Privacy [NBT 04])

6.3.4 Low ICT skills and the privacy divide

However, not everybody has sufficient ICT skills to protect their privacy. As an analogy with the "digital divide", there appears to be a privacy divide: those who know and act accordingly, and those who don't and remain vulnerable. Privacy is therefore not only an individual, but also a societal issue. A significant privacy-divide between average users and those willing and capable to protect their privacy would be the consequence of a policy relying mainly on individual behaviour. Moreover, the right to privacy is not equally divided. For example, children have little privacy rights as individuals, and are not consulted when their parents want to put up webcams in their nursery school. They should also have some rights to privacy.[32]

---

[31] http://www.habbohotel.com
[32] Electronic Surveillance [DBT 2000].

6.4 Concluding remarks

Privacy is context dependent. Absolute privacy is not a real option for human beings. Total confidentiality would exclude people from any network, i.e. social interaction in general, while total exposure would leave people too vulnerable. A choice needs to be made somewhere in the middle, between gaining easy access, security and services on the one hand and being watched and perhaps abused on the other. The right of informational self-determination is the basis of modern democratic societies. Each citizen should have the right to decide who knows what about him/herself and who is using what data, to what purpose.

In the “real world” we decide on a case-to-case basis what personal information we wish to share with other people, depending on our sense of trust. The challenge is to find a way to reflect this context dependence in the digital world. Our previous experiences cannot necessarily be “translated” directly into the digital world, because ICT poses different possibilities and boundaries. For instance, information (pictures, text etc) published on a weblog or in news group is potentially accessible to anyone, for an indefinite time. Modern society is more open concerning personal issues than we are used to historically, most people have low privacy awareness, and they lack technical and social ICT skills to counteract threats to privacy.

Chapter 7 Convenience

By Ida Leisner (DBT) and Johann Cas (ITA)

7.1 Issue at stake:

The widespread uptake of ICTs such as Internet, mobile phones and smart cards is largely a result of their convenience and usability. Not many people would go for the benefits of security, efficiency, service or social inclusion that these technologies provide, if it wasn't easy. But when using our credit cards or surfing the Internet out of convenience, the individual also leaves vast amounts of electronic traces and personal information. These personal information and electronic traces are generated and may be collected for marketing purposes, for paying bills, for investigating crime etc, and there is a risk of privacy intrusion. The issue of the trade off between convenience, usability and privacy will be discussed in this chapter.

Different individuals and stakeholders have different purposes for using ICTs, the context of use varies – and therefore they also tend to have different attitudes to ICT and perceptions of convenience and privacy. Convenience and usability are important for the individual user – whether it be as consumer, citizen or employee. The private sector tends to focus on efficiency and increased profits. They award importance to privacy primarily to maintain good customer relationships, as well as to comply with legislation. E-government institutions tend to prioritize efficiency in order not to increase public spending, but these institutions also intend to balance efficiency needs with privacy-legislation.

Though the loss of privacy is related to individual rights, there might be consequences for the society as a whole if privacy is traded off with convenience.

In many situations individual users accept the trade off between privacy and convenience, either because of lack of understanding of the implications of loss of privacy, or because measures to protect privacy are too complicated. In some cases this acceptance is not a voluntary one but enforced, as privacy respecting alternatives are not available at all.

The potential for privacy intrusive effects is not limited to the use of technologies – it may be a calculated risk: Some will be happy to trade their personal information or subscribe to direct marketing in return for a benefit such as a gift, bonus points for air

travel g. A recent Norwegian survey[33] showed that 14%, and 27% of youngsters have given away information in return for a free service or good offer. There is always a trade off, but it is not always transparent. Generally the individual user is not fully aware of the consequences of the trade off between convenience and privacy. The consumers and citizens seem to be little aware of the increasingly invisible and hence unnoticed collection of data, their transfer and use in different contexts, and the time spans between collection and use. Also data mining is mostly a hidden and unknown activity (Data Prevention [ITA 2002], Data Mining [ITA 2002]). The individual is no longer in control of their personal information and the extent of the original trade off is unknown. The (lack of) transparency issue is crucial for the individual managing the trade off.

In the EPTA projects we considered the trade off between convenience and privacy both from the consumers' points of view, and the citizens'. The consumer considers the trade off from the purely individual perspective – "what benefits will I receive" – while the citizen also assesses possibilities and threats in ICTs from a societal perspective. When citizens participate in technology assessment projects they tend to have a democratic interpretation of their role, and they will reflect on the consequences not only for themselves but for other members of society, such as the underprivileged.

7.2 Technological developments

The trade off between convenience, benefits and privacy will be illustrated in some examples of ICTs that are also described in appendix A.

7.2.1 Internet cookies

The Internet provides easy access to knowledge and web-services such as buying train tickets or checking the weather forecast. Being a frequent user of a certain service, it might be convenient to have personal information and preferences stored in cookies, so that next time the user visits the webpage, the service will be customized. This information can also be used for direct marketing, which some might consider convenient, and others might not. There is lack of openness about what the information is used for and a potential for surveillance.

7.2.2 Mobile phones

The mobile phone is probably the most popular gadget and tool for social inclusion, particularly for young people, who organize their social life and communicate via SMS. Carrying a mobile phone without being connected doesn't make sense, even though it

[33] Inger Anne Ravlum (2005): *Pinning our faith in Big Brother… and all the little brothers too?*, TØI Report 789/2005 for The Ministry of Modernisation, Norway

might be the best privacy solution. For parents, giving their children a mobile phone means being in touch with them no matter where they are, and thus creating a feeling of security. This security may be only perceived, since the parents are not in the same place as the children and thus unable to protect them. The possibility of being always connected could also mean unnecessary surveillance of the children (Electronic surveillance [DBT 2000]). (ICTs and social inclusion is further discussed in Chapter 6).

In general, mobile phones leave electronic traces; data retention as part of anti-terror-legislation has increased the electronic surveillance of mobile communications.

7.2.3 Location based technologies

Based on GPS technologies a variety of technologies and services connecting a user/item to a specific place are entering the market. The possible tailoring of information to the individual user can be convenient in situations such as route-finding or, swift emergency assistance on the basis of information location data from mobile phones. The privacy threats vary with the extent the user is controlling third party access to information about where he or she is or has been (Electronic Traces [NBT 2005]). (This is further analyzed in Chapter 4).

Location via GPS may not necessarily impinge on privacy if the position signal is processed offline (as is the case in standard GPS navigation devices or PDAs, where the additional information necessary to provide useful services like maps and points of interests are stored on the portable device. However if the position signal is sent to a service provider who sends back the requested information (usually mobile phone based systems), then privacy can be compromised. Intermediate, privacy friendly systems are also possible, for example adding real-time content to static maps by broadcasting road and traffic conditions over normal radio stations and feeding this information into car navigation systems.

7.2.4 RFID tags

It is argued that functional RFID-tags in food, clothes, et cetera, could be of convenience for the customer. For example it will help him or her find lost items at home and checking if perishables inside an intelligent refrigerator are within date. (Electronic Traces [NBT 2005]).

We know little about how customers will adopt this new technology. A recent investigation has shown that customers are very concerned about companies using RFID-tags for collecting data on consumer behaviour, but they will buy products with

RFID-tags if it for instance means improved food security or reduces risk of theft.[34] This illustrates the different interpretations of the trade off between privacy and convenience depending on the purpose and context. (Electronic Traces [NBT 2005], RFID [POST 2004]). (RFID-tags are further discussed in Chapter 8)

7.2.5 Privacy enhancing technologies (PETs)

Privacy Enhancing Technologies (PETs) are being developed to prevent the monitoring and recording of our social behaviour when using ICTs. These technologies can in principle protect personal privacy considerably. However, their practical deployment often requires advanced know-how, reduces the accessibility of services and slows down performance. It also involves additional costs for software and/or services and additional time invested in learning. Moreover, PETs are insufficiently supported by current regulations; in particular it is not compulsory to provide the option of anonymous access to services or infrastructures.

The Norwegian focus group study show that the inconvenience of using the privacy protection measures in the browser can be a reason why people are not doing more to protect their privacy. The same goes for encryption of e-mails – it is troublesome, and not considered necessary when posting non-sensitive information. The users said that if they were to use a program for encryption of e-mails it would have to be very simple to use.

In 2002 ITA did a detailed study on existing privacy enhancing technologies. The aim was to assess the usefulness of commonly available advice, searching for a possible reason for the observed divergence between expressed concerns about privacy and actual behaviour and identifying areas where individual responsibility cannot sufficiently preserve privacy. Two virtual users, one of them being a very privacy aware person, following all the recommendations usually given, the other one representing a person without any privacy concerns, had to fulfil the same list of frequent Internet activities. Their experiences and the problems they faced in doing so were compared and analysed and the data traces generated were observed.

The experiment showed that digital life becomes a lot more complicated when following the directions for maximum privacy. Implementing privacy protection measures can be a very frustrating user experience at the computer, and such frustrations have to be taken into account when assessing convenience. The technical problems ranged from “from minor inconveniences to the inability to access or use certain services”. (Private Internet Use [ITA 2002])

---

[34] Capgemini (2005): *RFID and consumers*

It seems, therefore, that at this moment not much should be expected from PETs unless more support and development efforts are devoted to them. For widespread use by normal users, they would have to become much simpler to use.

7.3 Social and cultural developments

The participating citizens in both the Danish and the Norwegian studies were willing to accept the trade off between privacy and convenience. The Norwegian study shows the consumer attitude to the trade off between privacy and convenience, while the Danish study focus on e-government/ digitalisation of administration, including assessing the societal benefits of e-government. (This perspective is further discussed in Chapter 9).

The Danish citizens can be described as “pragmatic and unconcerned” about their privacy (The municipality on the Internet [DBT 2000]). They were in general positive towards 24-hour electronic self-service, having access to the municipality independently of time and place. They argued that risks must be taken in order to increase convenience of ICT use. But the citizens also stressed, that in return for their willingness to give personal data, they expected transparency in data processing.

Digitalisation of public administration, which provides new services such as automatic regulation of taxes and social benefits, also means improved efficiency in uncovering social fraud. The citizens would accept this “bonus” from becoming more transparent as a benefit for the whole society, though theoretically they did fear “big brother” scenarios.

The Norwegian citizens (Attitudes to Privacy [NBT 2004]) are more concerned about convenience and usability than privacy. Surfing the Internet or using mobile phones, they might be sceptical about the risks, but they were willing to make a trade off and give away personal information, if convenience or getting something in return, such as a gift or free SMS messages was an option. They hardly ever read privacy policies, because they saw it as too time consuming and therefore inconvenient.

Both for the Norwegian consumer in the focus group interviews, and the Danish citizens in the lay panel the tendency are, that the more aware of privacy intrusive risks, the less motivated to trade privacy for convenience. The Norwegian study shows, that having competences for using ICTs in very advanced ways is not necessarily combined with knowledge about consequences.

When ICTs are used for crime or terror fighting, the citizens generally trust public authorities to handle their data properly. The Norwegian consumers showed great

confidence in the government and large Internet service providers, and Danish citizens pointed to the benefits of "friendly control" from public authorities. These results are in line with recent questionnaire-surveys in Norway[35] and Denmark[36]. The Norwegian survey showed that citizens have trust in both private enterprises, particularly banks, and in public authorities and have little fear of misuse of their personal information. They trust that privacy is well protected in legislation and by law monitoring institutions.

When assessing the consequences of the trade off between privacy and convenience one must bear in mind the importance of trust. To maintain trust points to keeping democracy strong and vivid. A Danish citizens' panel assessing the threats and possibilities in electronic surveillance put this societal approach forward. They found it important not to develop a society where suppression of crime, fraud, and terrorism is obtained as a result of surveillance of the individual. (Electronic surveillance [DBT 2000])

Do citizens and consumers want to protect their privacy, even if it means less convenience and usability? The answer from the Norwegian consumers and the Danish citizens tends to be a no. An answer not only due to convenience but also lack of awareness of the collection and processing of their personal information, and lack of usability in PETs meant for protecting privacy.

Empowerment of the consumer and the citizen is the "mantra" of recent attempts to manage the privacy issue at the individual level. One could argue that the trade off between privacy and convenience always is at stake and cannot be eliminated simply by empowerment of the individual - empowerment meaning not only the right of informational self-determination, but also the individual control over when privacy should be traded off for conveniences and benefits.

Protection of privacy rights is an important task for government, as well as ensuring trust – to make individual empowerment possible. Legislation, regulation and control as well as awareness programs should provide the (informational) ground on which the citizen can choose when to accept the trade off between convenience and privacy. The privacy protection must operate at two levels – the protective state and the empowerment of citizens and consumers. Only a mix of law, self-regulation procedures and individual awareness will help to ensure privacy in developed information society.

---

[35] Inger Anne Ravlum (2005): *Pinning our faith in Big Brother… and all the little brothers too?*, TØI Report 789/2005 for The Ministry of Modernisation, Norway

[36] ACNielsen (2005): *AIM for Det kriminalpræventive Råd*

7.4 Political and legislative developments

The development of privacy intrusive technologies is currently faster than the development of privacy protection measures. Many technologies are privacy intrusive in ways the user might not know about or understand. As new technologies continuously emerge, legislation will always have a tendency to lag behind. It seems there is a need for strong law enforcement in the field of ICT and privacy, for raising awareness of privacy and security matters.

In 2005 a proposed Danish law/bill suggested that informed consent should not be required as long as personal data are shared among different departments *within* the municipality. It was argued, that it would be more convenient for the citizen not to have to give consent over and over again for this data sharing. The law/bill is part of a reform that aims to implement the ”one-stop-shop principle” for e-Government, discussed in Chapter 9. The rules were tightened up regarding consent before the final approval in parliament, but there is still a gap between existing data protection rules and expected consequences of digitalization. This example shows that the legal protection of privacy is under heavy pressure, when even public authorities argue that data protection measures impede the provision of effective services.

Ensuring that legislation addresses the privacy threats associated with new technologies is a considerable challenge. The Norwegian study on Electronic traces (Electronic traces [NBT 2005]) mentions that while communication/traffic data must be destroyed after a certain period, this is not the case with location data. Similarly if RFID-tags are used to store personal data, the retailer must obtain a written consent from the consumer, according to the Data Protection Act. But it is not clear to what extent the Act would limit activities such as monitoring consumer habits while in a store (RFID [POST 2004]).

7.5 Concluding remarks

At present there seems to be a conflict between privacy and convenience, where convenience “wins”. There are different explanations for this. One is that technical solutions (so called “PETs”) to achieve privacy are relatively unknown and also inconvenient for users to use. Another explanation is that individuals are not fully aware of the implications of giving away personal information. Many ICTs are privacy invasive in ways that are unknown for the user.

In this arena, there is a need for stronger law enforcement as well as a greater awareness on the part of the individual citizen. In order to meet the challenges we need regulation at the national and the EU level, in combination with educational strategies to raise citizens’ awareness. In order to succeed, convenience must be given a high priority when assessing alternatives to not protecting privacy. If PETs are difficult to use, people will stop using them, even though they might realize that it does not serve their best interest in the long run.

Chapter 8 Economic benefit

By Christine Hafskjold (NBT) and Danielle Bütschi (TA-SWISS)

8.1 Issue at stake

Information and communication technologies are used in many business processes, in order to increase efficiency or create new economic opportunities. Customers can shop without cash, shop on the Internet, obtain information on new products via e-mails, receive discounts when using customer cards, etc. However, as more and more digital services are set up in business and commercial processes, each and every one of us leaves a dense network of data traces behind. In return for the benefits of digital services, we reveal a lot about ourselves: which suppliers and which brands we prefer, where we have recently been, or shopped, or paid a hotel bill, whether we systematically select cheaper goods or can afford more expensive goods, which internet pages and services we are interested in, etc. And, very often, we also reveal our personal data such as names, sex and place of residence.

All these traces are of great interest for commercial and business actors. Various TA studies undertaken by EPTA members' organisations identified three types of actors that use personal information for business and commercial purposes:

- Commercial actors that gather personal information, surfing and buying patterns for use in their customer relationship management, in marketing or to sell to other actors;
- Distributors of spam that collect e-mail addresses from chat-rooms, web sites and mailing lists;
- Companies that use personal information to verify the customer's access to a service, like DRM (Digital Rights Management), and thereby obtain access to excess information about the customer.

New information and communication technologies clearly offer new business and commercial opportunities, and it is legitimate that economic actors take advantages of these. However, these advantages can threaten privacy rights. In this chapter we shall look in more detail at the trade-off between privacy and commercial opportunities offered by ICT systems. We will consider the technological developments at stake, as well as the way these may influence society and the possible solutions for protecting privacy rights.

8.2 Technological developments

When surfing the internet, downloading software, shopping online or using a mobile phone we leave different traces that can be of interest to commercial actors. As a

result of the technological developments in ICT, it is virtually impossible to perform everyday tasks without leaving information about who we are, where we are and what we like. Understandably, some see the value in this information and wish to use it commercially. The problem is that it is not always clear to the user when he/she leaves traces or how a business will handle the information given to them – whether as direct input or electronic traces.

8.2.1 Internet use

When a user visits a web site, the owner of the web site can track the user's behaviour and surfing patterns through the IP-address of the computer, the URL the user has visited before and by different types of cookies[37]. In most cases the user has no knowledge of how this technology works, and is unaware of the traces that he or she leaves behind.

Even if the user does not log on to the website, the site owner can use the traces for statistical purposes. But if the user can be persuaded to log on to the site he or she visits, it gets more interesting. The information can then be mapped to a person, and not just an anonymous computer (Electronic Traces [NBT 2005]).

8.2.2 Data Mining and customer loyalty cards

Internet and e-commerce have made it easier to gather process and exploit consumer information. It has become much easier to trace individual customer's shopping patterns and preferences. Tailor made advertising and CRM (Customer Relationship Management) are becoming the rule rather than the exception.

Data mining is a label for technologies for finding useful patterns and rules within a large amount of data. Data mining can detect unknown relationships in data. Because of this, businesses can be tempted to gather as much data as possible, not just the data they need for a specific purpose. Because data mining is an activity mostly hidden from the consumers, the way it's used to influence their behaviour is completely non-transparent (Data Mining [ITA 2002]).

Data mining is interesting to businesses because it can give them detailed information about their customer. By analysing the data they can find out which customers are the most profitable, which product placements are the most effective, what customers pose the biggest risk etc. This could violate Article 15 of Directive 95/46/EC on "Automated individual decisions" which states that persons should not be subject to decisions based solely on automated processing of data (Data Mining [ITA 2002]).

[37] See Appendix A – Overview of Technologies for a detailed technical description

The issuing of special offers, only available to desirable customers, could also contribute to a two-class society (Customer Data [TA-SWISS 2000]).

One way of obtaining detailed customer information for businesses where most of the shopping is performed in the real world is by issuing customer loyalty cards. The customers provide personal information – register – in exchange for special offers, general discounts or similar offerings (Customer Data [TA-SWISS 2000]). Through the use of the card, the companies can register all purchases from the customer and the information can be analysed in their data warehouse. By partnering with a credit card company, so that the loyalty card also can be used as means of payment, the business ensures that the card will be used every time the customer shops.

8.2.3 Adware/Spyware

Spyware are programs that are installed to the users' computers without their knowledge. Adware are programs that display commercials for the user. Both types of programs often come bundled with free software. With adware the user may have been warned about this in a licence agreement, but these agreements are often long and written in a language meant to conceal the nature of the program to the user (Electronic Traces [NBT 2005]).

Spyware programs can have different uses: Some gather information from the user's PC and send it back to the company responsible, some open back doors to the computer, some are keystroke loggers and some are programmed to hijack the user's browser and change the settings. In many cases the programs slow the computer down and even cause it to crash. Sometimes Spyware and Adware blend into one another, as the pop-up windows with advertising also have code to change the user's browser settings, or to make it virtually impossible to uninstall the software.

In a testimony before the US Senate Committee on Commerce, Science and Transportation, the organisation Centre for Democracy and Technology (CDT) lends some insight into how spyware and adware work[38]:

> *What the growing array of invasive programs known as spyware has in common is a lack of transparency and an absence of respect for users' ability to control their own computers and internet connections.*

In theory the business model of adware is quite simple: An advertiser pays an adware company to place their advertisement in their program. The advertiser typically gets a

[38] Center for Democracy and Technology (2005): *Testimony of Ari Schwartz, Associate Director Center for Democracy and Technology before the Senate Committee on commerce, Science and Transportation on "Spyware".* http://www.cdt.org/testimony/20050511schwartzspyware.pdf

commission pr. click. The adware company pays a distributor to bundle their program with a software program and in turn gets their commission pr. installation. This means that a lot of money can be made on commissions if the number of installations and clicks can be maximised. Using code that downloads the software automatically without the user's knowledge is therefore tempting.

In an article in Wired news (December 2004)[39] it's claimed that some consumers actually accept spyware willingly as a means to "pay" for freeware that they find useful. But for the majority of the consumers, adware and spyware are perceived as annoying, intrusive and often damaging to the computer.

8.2.4 DRM – Digital rights management

Digital rights management (DRM) is a relatively sophisticated form of protecting digital intellectual property, whether we are talking about film, music, a computer program, a presentation or a report. With DRM you have to be authenticated to obtain access to contents that you have legally bought. When shopping for music you do not only buy the song you want, but also choose the kind of access you want to the song: Do you want to listen to the song only once? Do you wish to save it? Do you want to be able to copy it for use in another media? The authentication process checks what kind of access you have paid for, and makes sure this is what you get.

Most existing DRM solutions require that the user identifies themselves in order to prove that he/she has a right to access the content in question. This limits the opportunity for anonymous use of content and facilitates the compilation of profiles with detailed information about a person's preferences in music, film and other content (DRM [NBT05]).

8.2.5 RFID

Radio Frequency identification (RFID) is being widely investigated not only as a means of crime reduction but as a means of increasing supply chain efficiency: RFID tags are already widely used in applications like animal tagging, electronic transport (e.g. transport for London "oyster cards") or supply-chain optimisation, but can also be used to record detailed buying patterns, e.g. how the customer moves around the store (RFID [POST 2004]).

Still the price of the tags is too high for them to be widely used on individual products for consumers. However retailers chains such as Wal Mart are launching pilot projects for stocktaking purposes. Other large supermarket chains are experimenting with

---

[39] Delio, Michelle (2004): *Spyware on my machine? So what?* Wired News. http://wired.com/news/technology/0,1282,65906,00.html?tw=wn_tophead_1

RFID tags on expensive products, primarily to prevent theft. It is predicted that when the tags become cheap enough, the RFID tags will be used as bar-codes, enabling the products to be registered and the total price calculated when the customer passes through check out.

The main privacy concerns regarding RFID tags are related to the following (Electronic Traces [NBT 2005]):

- use of data by a third party
- an increase in direct marketing
- the ability to track individuals through the products they carry
- the ability to "profile" individuals through the products they carry

Currently the potential for tracking a person based on a product with an RFID tag is limited because of the lack of global standards in this area. Technologists also argue that the tracking of individuals will always be difficult because of the large amount of power needed to read RFID tags at a distance (RFID [POST 2004]). However, if the density of readers is sufficiently high, a fairly detailed picture of a person's movements can be made, even if the person can't be traced continuously.

8.2.6 Location-based services

Use of GPS is becoming increasingly popular, particularly in navigation systems in cars, but also as a built in feature of mobile telephone. In the US, the government has directed all mobile network operators to be able to locate their users, so that 911-callers can be found. Use of GPS in mobile phones has been seen as one way to meet this demand. In Japan, all mobile phones are required to have GPS by 2007.

Determining the location of mobile phone users is not just done for security reasons. Many operators also offer services like fleet management (for transport companies or companies with a big sales force), map services for cities, "find your friends", etc. Today, most of these services are based on data from base stations, and not GPS (Electronic Traces [NBT 2005]).

Many such location-based services are conceivable and belong to the vision of pervasive computing (Pervasive Computing [TA-SWISS 2003]). The challenge with services like these is that it's easy to abuse them, so that something that is meant to be useful or fun turns in to surveillance: If you use the phone as part of the fleet management system – how do you know that the boss isn't watching after hours? For the "find a friend" types of services, mutual consent is required – but how do you ensure that no one accepts the service on your phone in an unguarded moment? Should parents be allowed to keep track of their children using a service like this?

8.2.7 Spam

The posting of e-mail addresses on websites, in chat rooms and through filling in various forms on the internet, leads to the spread of these addresses to various distribution lists. Once on one or more of these lists, spam is virtually impossible to get rid of, even with a good spam-filter (Electronic Traces [NBT 2005]).

Better search engines make it possible to scan an increasing number of web pages and chat rooms in search of e-mail addresses to add to the lists. Research conducted by the Center for Democracy and Technology (2003)[40] shows that e-mail addresses posted on Web sites or in newsgroups attract the most spam.

Spam isn't just annoying; it's also a big expense. Spam filters cost money and take time to install. Employees use time to sort through and delete spam, and even the spam that is caught in the spam-filter steals bandwidth. In addition, spam can contain viruses and spyware/adware. A few years ago you were safe as long as you didn't open any programs that didn't come from a credible source. Now, files can be installed on a computer if only the opened or previewed e-mail contains a picture, banner or other image. The user does not have to click on the image or install anything.

This makes spam even more dangerous than it was before, and this also has an effect on companies that send out newsletters or offers that their customers have subscribed to: To avoid viruses and spyware, the security conscious user will have disabled images and other "dangerous" file types. Thus, the marketing effect is reduced.

8.3 Business and commercial developments

8.3.1 Customer relationship management

All direct marketing is based on information about the customer. The minimum information necessary is a name and an address (or e-mail address), but the more detailed the information, the better from a marketing point of view. Sending brochures and similar material to large, diverse groups is costly, and you may not get the desired effect. By collecting or buying demographic data, and information on people's interest and behaviour, the marketing could be more efficient as you can send tailor-made advertisement to your customers. This is so-called customer relationship management, a new way of doing marketing.

From a consumer point of view, this new marketing philosophy can be seen from two sides: On the one hand, it seems like a good idea to only get advertising for products

[40] Center for Democracy and Technology (2003): *Why am I getting all this spam?* http://www.cdt.org/speech/spam/030319spamreport.shtml

that you are actually interested in, and not for all other products. On the other hand, most people will not be comfortable knowing that their grocery store or consumer electronics chain has detailed personal information about them. For the companies the challenge is to uphold the balance between collecting information for marketing purposes and respecting their customers' privacy. This seems to be best done by not asking for information on a level that the customers will find intrusive (e.g. information that seems unnecessary), and by upholding a strict privacy policy. The latter involves storing the data in a secure way, not using it for other purposes than stated in the security policy and not reselling the data to others.

8.3.2 Spamming

Marketing also means communicating to a maximum of persons. New ICT developments offer almost unlimited opportunities to send advertisement to potential customers, and spamming has become a new economic branch. The companies that distribute spam normally get paid per hit. The technical development makes it possible to send spam to an increasing number of e-mail addresses faster. This makes it profitable to do this even though the hit rate (the number of people actually clicking a link or buying a product as the result of spam) is low.

8.3.3 Free software

Many free services or software products depend on income from personalised advertisements or the trade of personal data (Telecom and Internet [ITA 2000]). Some software vendors, for instance, offer two versions of their program – one that you pay a licence fee for that comes without advertising, and one free version that comes with advertising. The customer thus chooses how he or she wants to "pay" for the software.

Other distributors of free software work with adware companies. If the adware company is law-abiding, this can be unproblematic, but adware is known to be a source for spyware, as described in the previous chapter.

8.4 Social and cultural development

8.4.1 Limited awareness

Research such as the Norwegian focus group study indicates that the public has very little awareness when it comes to the use of ICT in commercial and business processes – they don't know that their behaviour is being monitored, they don't see the value their personal information can have to others and they never considered that the company they gave their information to might sell it to someone else (Attitudes to Privacy [NBT 2004]). And even when users do know about the traces they leave, the

willingness to make an effort to do something about it is limited. This is supported by a larger study founded by the Norwegian government that shows that people generally trust the companies and institutions concerned, to respect their privacy.[41] However, various foresight studies point to a future where consumers are more privacy-conscious. The opposition towards RFID tags seen in recent years has already forced companies such as Gillette or Wall Mart to limit their plans for widespread tagging and to reconsider their strategies. In this respect, even though awareness to privacy is low at the moment, companies that take their privacy policies seriously might develop competitive advantages.

Another challenge is that the products and services that can help users protect their privacy in general are unknown and not very user friendly. Some of the services that were formerly available as alternatives for those who wanted to be anonymous are disappearing, either as a result of increased focus on national security, or for financial reasons. Examples of are the banning of anonymous cash cards for mobile phones (security reasons) and putting up toll booths that are unmanned, where all cars are photographed and then billed.

Low awareness is not only a problem with the individual users. It's also important to focus on the awareness of the people who handle the information. Companies that take their customers' trust seriously should make sure that personal information is stored and handled in a secure way. For instance, in June 2005, a hacker gained access to detailed information on 40 million credit cards. It turned out that not only was the information not properly secured, but also the company in question did not have permission to store this kind of information.[42]

8.4.2 People don't place a value on their personal information

The NBT focus groups had not given much thought to what happened to their personal information, and were appalled to learn that some companies sell on their customer databases to others. After receiving information about electronic traces the members of the groups were more sceptical towards giving information about themselves when prompted for it. But many of them admitted that they would do it if they were offered something in return (a gift, free SMS/MMS messages) (Attitudes to Privacy [NBT 2004]).

[41] Inger Anne Ravlum (2005): *Pinning our faith in Big Brother… and all the little brothers too?*, TØI Report 789/2005 for The Ministry of Modernisation

[42] Sahadi, Jeanne (2005): *40M credit cards hacked. Breach at third party payment processor affects 22 million Visa cards and 14 million MasterCards.* CNN. http://money.cnn.com/2005/06/17/news/master_card/

8.4.3 Nobody reads privacy policies

In the Norwegian focus group study, it was found that people did not bother to read privacy policies on sites they visited, as they found it too time consuming. They assumed that reliable companies would respect their privacy (Attitudes to Privacy [NBT 2004]).

There are also examples of companies using the fact that people find privacy policies and licence agreements long and tiring to do questionable things in a legal way. As long as they can get the users to press the “I agree”-button, they are protected from lawsuits. In LA Times, Joseph Menn cites an example of a well known adware company, Claria Corp. A Claria licence was more than 60 electronic pages, and didn’t mention "pop-ups" until page 18![43]

8.5 Political and legislative development

8.5.1 Data gathering and data protection

In most European countries, companies are not allowed to use personal information unless they have the person’s consent or the use is stated in a law (the reporting of certain statistics for instance). Moreover, companies have a special responsibility to ensure sufficient security for sensitive data. In addition, a business has a duty to give information on what data they have registered about a customer/user, and how the data is secured if the customer/user requests it.

Most data gathering activities are subject to data protection law (see Chapter 3), but it is very difficult to enforce, and therefore it is unclear to whether there is full compliance with the law across the electronic sector. For example in the UK, enforcement of data protection law by the Information Commissioner is largely reactive – i.e. responding to complaints, and therefore depends on consumer awareness of the law. And in Switzerland, the Information Commissioner’s main mission is to advise and inform. Complaints have to be addressed to regular courts.

8.5.2 Spam

Most countries have laws against spam, and there is a trend towards enforcing these more strictly. However, the global nature of the internet makes the enforcement difficult, as servers can be placed in countries with a more relaxed attitude.

[43] Menn, Joseph (2005): *No more Internet for them*, LA Times. http://www.latimes.com/business/la-fi-fedup14jan14,0,111456.story?coll=la-home-headlines

8.5.3 Intellectual property rights

EU directive 2001/29/EF gives directions on harmonisation of different aspects of intellectual property rights and rights in the information society. In Norway, the recommendation from the Parliament committee is that consumers may break the copy protection codes if they have to in order to play their CD on “relevant equipment”. This means that if you buy a CD that plays on the stereo in your living room, it should also play on your car stereo. If the copy protection prevents this, you may make a copy without the copy protection. According to the record industry, this problem will be short lived, as all intellectual property will use DRM technology in the future.

As for privacy, in their comment to the proposal from the Ministry, the Parliament committee only says that the Ministry should make sure privacy interests are attended to (DRM [NBT 2005]).

8.5.4 Consumer pressure

A study carried out by Consumers’ International on “Privacy and the Internet” found that legislation may be most effective when combined with consumer pressure – for example although there is privacy legislation in the EU, a large number of websites do not comply with the directive, partly due to lack of consumer pressure (Electronic Privacy [POST 2002]).

8.5.5 Legislation lagging behind technical development

Technological developments will continue and legislation is bound to lag behind. RFID for tracking persons and goods provides an example. Currently their capabilities are limited because of their costs and of the lack of global standards: a tag produced by one company could not necessarily be read by another. Furthermore, the tracking of persons remains difficult because of the large amount of power needed to read RFID tags at a distance. (RFID [POST 2004]) But what will happen if these obstacles can be overcome? Will existing legislation be able to control personal RFID tracking?

8.6 Concluding remarks

The interests of private enterprises often differ from (or are in direct conflict with) that of the individual. This becomes clear when privacy and commercial interests are discussed. It is not always clear to the user what kind of traces he or she leaves, how and for what purpose private enterprises collect and process the data, and what value the data represents. Trade-offs between privacy and, for example, receiving a “free gift”, often occur in an unbalanced manner. A private enterprise may present a “Bonus card” as a symbiosis between the consumer and the company, when it in actuality it is an asymmetrical relationship, when the economic benefits to each party are considered.

“Adware” and “spyware” goes one step further by entering the user’s PC. This makes it even less transparent what kind of data is being collected, what it is used for and by whom. The user might accept an “End-user agreement” about the function of the program, but the consent is not necessarily informed. A different example is DRM technology. It is understandable that content providers are interested in protecting intellectual property rights - but again this interest might be in conflict with user interests in terms of convenience and the idea of free flow of information. Here DRM systems pose restrictions, which primarily benefit the interest of the content providers. RFID tags pose similar tensions and challenges.

Solutions are probably to be found in user awareness (consumers’ demand on private enterprises) in combination with regulation at the national or EU level. Present regulations should be re-examined to see if they are strong enough to encourage careful handling of personal data, and if the penalties for violating peoples’ privacy are adequate.

Chapter 9 eGovernment

By Stef Steyaert (viWTA), Ida Leisner (DBT) and Robby Deboelpaep (viWTA)

9.1 Issue at stake

ICT offers many possibilities for interaction between the public sector, on the one hand, and companies, institutions and citizens on the other. The term eGovernment is used by many countries and by OECD, to refer to the use of Internet to provide online services from the public sector, and also for other Internet based activities, such as e-consultation. Driving forces for rapid growth are the need for rationalisation and increased efficiency in the public sector and the (presupposed) need for an easier and wider access to public services for users.

It is necessary to make a distinction between ‘e-democracy - practices aimed at increasing participation processes,’ and, ‘eGovernment’ -practices aimed at ameliorating and modernising government (E-governance [viWTA, 2005]). There are several reasons for making this distinction: Fist, in most democracies there is a clear distinction of the different powers, the so-called ‘trias politica’: the legislative power, the judiciary and the executive power (generally called ‘the government’). Secondly there is a difference in goal: while eGovernment is generally aimed at improving public service and increasing efficiency in the civil service, e-democracy aims at improving consultation and participation to the decision process and thus enhancing democracy. Thirdly, the background processes and the technology, but also the societal aspects, differ.

Although there are clear links (f.i. in most countries the government is the driving source for e-democracy), there is a difference because of the different aims. And because of this difference, the privacy related discussion also differs. In e-government applications, normally there is no need to express one's values and political convictions. E-democracy by its very nature involves exposing personal beliefs and political ideas. Most of the projects discussed in this chapter deal with e-government, as E-government is a rapidly growing field and we see new activities in this area in most European countries. But even in this public area, the framework for privacy procedures and techniques stays rather generic. Except for specific areas such as justice, defence and public order (where there are specific privacy concerns), there is no specific framework for privacy procedures. This may be a cause for concern, particularly in some fields such as e-democracy, where a person exposes his or her political or ideological beliefs. And the introduction of electronic identity or citizens’ cards leads to new questions related to privacy (and the gradual introduction of biometric data on such cards imposes even greater threats).

There is no doubt that the ongoing evolution towards e-government and e-democracy, in development of applications (e.g. citizens card, digital municipalities) and of organisational systems (f.i. the use of the “one-stop-shop” principle, described below), has democratic potential and could improve public services. But there are issues to consider in the light of the privacy discussion, depending on which applications and solutions will be developed and used. In the following section, we will list some of these before proposing some possible solutions.

9.2 Technological developments

9.2.1 Infrastructure

The strategy for several European e-government-initiatives is to built an infrastructure, that ensures more freely availability of personal data, that can be reapplied anywhere in a service-oriented architecture (this goes for Denmark, Norway and UK and other countries). The idea is to create “one-stop shopping” in the public sector, where the citizen is only required to make contact with the system at one location, and from this location, all of their social service needs can be met. In addition, administration and casework can be more effective and flexible. This infrastructure can only come to existence by circumventing the legally defined “walls” between institutions and authorities to the benefit of creating one integrated administrative body. The trade off for convenient one-stop-shopping may be a loss of transparency in the public sector and possible threats to privacy (E-government [DBT 2005]).

9.2.2 Citizens’ Cards and Digital Signatures

One of the main drivers for citizens’ cards is the convenience of easy access to public information and services. In some cases electronic transactions may also be given preferential treatment. A general threat of citizens’ cards is that they encourage extensive use of secure access modes even for non-critical transactions. At the same time citizens’ cards and digital signatures allow also the provision of private or public services in a secure and privacy protecting manner.

In numerous European countries digital identification cards are in use (e.g. Austria, Belgium) or there are plans to introduce them (e.g. United Kingdom). Danish citizens have to use a digital signature in order to communicate electronically with authorities in a secure and privacy protecting manner. 10 % of the population installed the digital signature within the first three years of the programme, with a major increase when access to personal health records became possible. 10 % of the population has installed the digital signature within the first three years. Much of the increase in downloaded certificates came when access to personal health records became available. Despite this, the signature has proved less attractive than expected, due to the limited number of applications– but this situation is changing as more institutions accept the signature (E-government [DBT 2005]).

9.2.3 Identification versus authentication

Identification asks the question “Who are you?” – it is about finding out who (or what) somebody is based on specific attributes. Authentication deals with the verification of identity and asks the question “Are you who you say you are?” This is closely linked to identification (the process of checking whether the alleged identity is the same as the true identity). Authentication is normally done for one out of two reasons. In some cases it’s about restricting access to services or information, or the protection of resources. In other cases authentication of users allows them to be held responsible for their actions. Whether to authenticate and what type of authentication to choose certain service, is of great importance for privacy. It’s therefore important that the degree of authentication is fitting to the purpose, and that the method used is no more invasive than necessary (Biometric Passports [NBT 2005], E-governance [viWTA 2005]).

In the Austrian project on the Citizens’ card (Citizens’ Card [ITA 2002]), and in the Flemish project on ‘E-governance’ (E-governance [viWTA 2005]), experts highlight the distinction between identification and authentication. To keep the balance between the authorities’ need for information and the privacy of individual citizens, one should consider when identification is really necessary. A transparent system will enhance confidence, which is needed for the acceptance of e-government and e-democracy. A mediating institution (a so called ‘trusted agent’) could be helpful in this matter, e.g. in decoupling identification and authentication. The mediating institution assures that the identity of a person or institution issuing a request is correct and gives an authentication token (may take the form of an alias identity, but other techniques are possible) which is then be processed by the civil service or public authority (which can be sure that a validation of identity has taken place). Further authentication by the civil service or public authority may then take place (f.i. as to the authorization of the requestor to the requested information), the request is processed and the result transferred to the requestor. In such architecture, information and personal data are decoupled, although identity control has still taken place. The mediating institution can and should be monitored more easily by supervisory authorities (as mentioned in the EC Directives on processing of personal data (and should of course take the necessary security measures).

9.2.4 One card, several purposes

The ITA-project (Citizens’ Card [ITA 2002]) as well as the DBT-project (Citizens’ Card [DBT 1994]) on ‘Citizens card’ illustrates the problem between the one purpose card and, the multi-purpose card (for identification, e-government, social security, health

data or commercial purposes)[44]. The former has greater potential to fulfil the transparency requirement, while the latter has more economic potential and will increase efficiency. Citizens are in favour of separate cards because they find it important to distinguish private, public and commercial purposes. But separate cards will have an impact on cost-effectiveness. At individual level, this will increase additional costs for cards (and readers). Furthermore, it is clear that some parties would value the possibility of combining data that a multi purpose card would offer (e.g. banks). So, in the case of multi-purpose cards, measures need to be taken to prevent improper use. This means a higher complexity of the mechanisms (hardware and software) to prevent such improper use and some organisational innovations, which will reduce acceptance even further.

9.3 Social and cultural developments

A literature study carried out by viWTA (E-governance [viWTA 2005]) shows that attitudes to privacy vary culturally and historically, so it is hard to find one precise definition of privacy. In the traditional approach of democratic societies, privacy is considered a basic human right. It is associated with values such as independence, freedom of movement and speech, self-respect and integrity. But these values are hard to quantify when evaluating potential privacy implications of ICT. For such evaluations, many studies suggest using more substantial criteria such as the purpose, usefulness and necessity of data collection and gathering (see Chapter 3 – the fair information principles). Transparent procedures are also of key importance in building and maintaining trust.

In Denmark, citizens are generally happy with their personal data being registered and processed, because they trust public authorities. This trust doesn't seem to be diminished as new technologies enable further control and registration of citizens. In 1994 Danish Citizens advocated against a Citizens Card to be used for both public sector purposes and banking, insurance and other private sector purposes. Today Citizens may not be unconditionally against such an integrated solution.

In other countries with a different historical background one might expect a different attitude to personal data being filed in databases.

9.3.1 Pragmatic AND unconcerned

The results of the project ‘Municipality on the Internet’ (Municipality on the Internet [DBT 2000]) and ‘Citizens card’ (Citizens’ Card [DBT 1994]) showed that citizens are ‘pragmatic and unconcerned’ when asked how they feel about e-government

[44] In Denmark a number of governmental parties have joined in doing a business case on the multipurpose identity card. The case shall not (underlined) include commercial solutions. The business case for decision is ready in February 2006.

applications (such as administrative operations through the internet). Pragmatic because, in their opinion, you can't stop the development, so you have to get the best out of it. The Danish citizens were not against giving information including their personal identification number via the Internet, provided it was safe and secure - and today most Danish citizens trust the public authorities. In general, citizens are very positive about the new possibilities. And, as for privacy, citizens see a trade-off between the need for privacy on the one hand and on the other hand, the user-friendliness of the systems. But, while being pragmatic and positive, they stress the importance of having the right to gain insight into, and control of, what is done with the information they give to the authorities. A similar conclusion is found in the viWTA project on the elderly and ICT (Colourful Flanders [viWTA 2004]), and in a recent project on privacy and citizen empowerment in e-government in Denmark (E-government [DBT 2005]).

Experts are much more concerned about privacy issues than citizens. In the DBT as well as the viWTA projects mentioned, experts declared that the generic privacy regulations are not sufficient and that privacy in e-government should be treated as a specific issue (e.g. inserting specific rules for e-governance operations to the existing legislation, such as the privacy laws, and adapting the organisation of the civil service, for instance to ensure privacy issues are well monitored and e-governance operation are properly processed). The central collecting and storing of data, often inherent in e-government applications, may create new threats in vulnerability and even enhance the risk of making faults in administration. Digitalisation increases the need for correct record keeping, as electronic documents are easily updated, exchanged, original copies may be lost, etc. (E-government [DBT 2005]).

Private information could leak to the wrong people or may be used in an unpredictable way; one aspect of privacy enhancement is to secure these data and to impede unauthorised access (e.g. to electronic health records) another is to increase transparency and to provide people with access to their own data, allowing them to correct these data if necessary.

Danish law experts recommend that

- the exchange of data between various administrative agencies/working areas in e-government should only occur upon a formal request for the disclosure of personal data (to avoid function creep).

- the use of "metadata" (descriptive data about other data) should ensure that the provisions in the personal data act concerning purposefulness and data quality are maintained during the repeated use of data.

- To put the citizens in control of their own data, IT systems should be designed in a way that citizens receive direct access to their own case journals.

9.3.2 E-government: excluding or supplementary

One of the main arguments for e-government applications is that it will increase the efficiency and effectiveness of public services. All mentioned projects prove that it will be impossible, at least for the coming decades, to make the e-channel the only possible channel for citizens to get in contact with their 'government' (whether it's local, regional or national). The viWTA project on ICT and elderly (Colourful Flanders [viWTA 2004]) very clearly shows that, although elderly people are very enthusiastic about the possibilities of different e-applications (including e-government and e-health), they demand that parallel circuits are kept alive. The 'e-way' never can be the only way. At the organisational level, parallel structures are necessary for physical as well as virtual contact. Citizens see the new technical possibilities as a supplementary service to the traditional system, not as a substitute to the system they have today. It's of crucial importance for them that the use of citizens' cards or similar services stays an option rather than a prerequisite for using public services. E-government should not cause a digital divide between citizens, depending on their ability to make use of ICTs.

9.3.3 Trust

Although the trust issue is not only an issue related to e-government and even privacy (as this is a broader societal and political issue), the trust issue is of particular relevance to e-government. In some international benchmarking studies on e-government, trust is seen as an essential element (whether in positive sense: a stimulant or in negative sense: a barrier) to the development of e-government.

There is a tendency to design e-government systems from "the inside out" (from the perspective of the public administration), and not the other way round: What architecture should we choose in order to give citizens maximum access in the user-friendliest way? While it is easy for e.g. the nurse to look into your EHR, it is not as easy for the citizen. This can create an informational unbalanced relation, in a situation where trust is crucial.

The Danish project on e-government (E-government [DBT 2005]) points to the lack of political focus on this issue. Transparency is a key element to increase citizens' trust and diminish the fear of privacy intrusion or misuse of personal data. It is therefore of crucial importance for realising the efficiency potential of e-government. Citizen's trust is based on experience rather than based on technical guarantees – and neither transparency nor trust is a predefined guaranteed outcome.

9.4 Legislative and political developments

Some e-government applications will conflict with existing legislation. Legislation is seen by OECD as one of the barriers to successfully developing e-government[45], e.g. to achieve the potentially increased efficiency of digitalisation. There is a risk that adapting legal framework to technological solutions in e-government will include defining data protection laws as part of the barrier. At least in Denmark there have been examples of this interpretation. Laws on specific data registers tend to undermine the general data protection act in making exceptions (eg giving up the demand for patients' informed consent on sharing data in a medicine profile register). Proposed laws on local governmental structure involve organisational changes that would facilitate e-government, but also threaten the citizens' basic rights to security and privacy. How this organisational change will be brought to reality is yet not clear. Danish law experts reacted by recommending that:

"Technology should be employed to make it easier for the citizen to give their *voluntary, specific, and informed* consent for the disclosure of data (instead of changing or making exceptions to the rules of consent; something that has happened in a number of cases)" (E-government [DBT 2005]). The experts consulted in the viWTA project on E-governance and privacy (E-governance [viWTA, 2005]) react in the same line of argumentation. Authorities tend to erode basic privacy rights in the light of efficient and effective e-government applications while they ought to be doing the opposite. Because of the specific nature of e-government and certainly e-democracy applications, they should even be strengthening privacy protecting measures.

Experts stress the need for a debate. Experts see a conflict between the protection of privacy and the cost-effectiveness of e-government applications. Citizens will expect a more transparent administration and public service and more and easier control over their own data. But this will conflict not only with insufficient regulation (e.g. regarding ownership of data) but also with inherent organisational, economical and societal consequences of ICT-applications (citizens' card) in this field. Applications like the digital signatures can also be used as privacy enhancing technologies instead of being privacy threatening. The experts also plead for a strategy to create more privacy awareness amongst policy makers, civil service and the general public.

9.5 Concluding remarks

Privacy is a double-sided issue. On the one side we need *secure* systems that can impede unauthorized access to e.g. electronic data records. On the other side there is the question of access to personal data and other technical means to increase

[45] OECD (2003): *The eGovernment Imperative*

privacy. Through, for example, access to personal e-government files, a citizen can verify the use, authenticity and accuracy, of his or her own personal data, and as a result, achieve a higher and more informed level of privacy and trust in the systems. This can made part of a strategy where e-government is used to empower the citizen.

The primary driving force for implementing e-government systems in recent years has been the need for rationalisation and efficiency for the public administration and convenience for the citizens. There are initiatives that take advantage of technology to give the citizens access to their own medical records for example – but in general privacy is not among the top priorities in the design of e-government solutions.

One of the reason is that modern e-government is built around a “Service Oriented Architecture” where the legally defined “walls” around public units are removed in order to ensure the flow of information which is deemed necessary to provide the required service. A central challenge is how the new technology can be used not only to increase efficiency for public administration, but also to strengthen privacy for the citizen - and create mutual transparency between public administration and citizens. There need not be a conflict between privacy and efficiency. Thus, the introduction of digital signature does not threaten citizens’ right to privacy per se, as long as it is applied with caution and awareness. In the case of e-government, a digital signature can even be considered a Privacy Enhancing Technology (PET). Whether the technology enhances privacy or not is largely dependent upon its specific implementation and whether or not the protection of privacy has been built into the design of the entire system.

Chapter 10 Healthcare

By Nicole Vouilloz (TA-SWISS); Danielle Bütschi (TA-SWISS), Stef Steyaert (viWTA)

10.1 Issue at stake

The use of Information and Communication Technologies in medical care is commonly referred to as “e-Health”. The developments in e-Health aim at achieving a better quality of medical care, possibly at lower cost, as well as at increasing transparency of the health care system. E-health is also expected to increase the availability of data for medical research.

On the other hand, e-health poses crucial questions related to privacy, as it deals with sensitive data, related to patients’ health, to their genetic make-up or other personal features. In this respect, privacy is an important issue to take into consideration in e-Health developments.

Privacy has ever been a crucial feature of medical practice. The medical secrecy is, in this respect one of the pillars of any medical activity. According to this principle, patients are the owner of their medical data and records: only patients can decide whether they want to transmit their data to third parties and at which conditions. With the development of ICT applications in the health sector, privacy is challenged, as there will be an increase in data exchange and new security threats might appear.

10.2 Technological developments

The development of ICTs in the health sector leads to a variety of applications. Considerable efforts are especially invested in the development of telemedicine, i.e. in the administration of treatments from a distance. Electronic health records (EHR) are also an important field of ICT developments within the health sector

10.2.1 Electronic health records (EHR)

Electronic health records are electronically managed health records. The potential advantages of EHR are more effective and secure treatment of the patient, due to the easy and rapid access to necessary and updated information about the patient, independently of time and place. This makes EHR a valuable tool for the healthcare professionals. EHR also offer major advantages for the health care system as a whole, as they facilitate and increase opportunities for evaluation, quality control and statistical analysis. In this respect, EHR not only offer advantages for patients and healthcare professionals, but they can also benefit to scientific research, to preventive medicine programmes or for the insurance companies. Furthermore, electronic health records mean that further uses of telemedicine can be envisages (see under).

All in all, EHR have the potential to increase efficiency of the health care system, a tendency that decision makers are looking for. Most European countries are investigating the possibilities to introduced EHR, in one form or in another. In Denmark, where the Danish Board of Technology organised a citizen conference on Electronic health records (Electronic Health Record [DBT 2002]), the national goal is to cover all hospital beds with an electronic patient record by 2006. This means that every patient going to the hospital will be registered in a personal record. The citizens, who were invited to give voice to their wishes and their worries concerning the digitalisation of patient records, described this technological trend as something that is "more than electrifying the old paper record; it will affect the relation between patient and doctor, the work sharing and organisation in hospitals and primary sector. And it will open a whole new range of possible use of data about the patients, introducing new treatment regimes …". This view is also shared by the authors of the Swiss report on electronic patient records (Patients' records [TA-SWISS 2000]), who highlighted the increasing networking possibilities this technology may induce and the changes in roles that may appear, especially for physicians.

In Switzerland too, several initiatives within hospitals and cantons aim at introducing electronic health records and a digital health card. In Geneva, for example, the e-toile project intends to connect all healthcare institutions via a medical information network, at the heart of which is the electronic patient dossier. This ambitious project is, however, facing political resistance, mainly for economic reasons. In Canton Ticino too, a HER project, "rete sanitaria", is being developed[46]. The issue is also discussed at the national level, but its ruling remains a complex policy problem due to the Swiss federal system.

10.2.2 Telemedicine

In a broad sense, Telemedicine describes all medical treatments occurring when the participants are not in immediate contact with each other. To close the physical gap between medical providers or between patients and medical providers, data and information are transmitted via electronic media such as email, or via conventional communication channels such as the post, telephone and fax. Telemedicine has thus wide range applications. For instance, thanks to telemedicine, medical advice is available, simply and around the clock, in medical call centres. In these centres, medically trained specialists, supported by a computer program, can give recommendations about what to do next or provide various information, such as the names and addresses of specialised practitioners. In more developed applications, tissue samples can for example be taken during the operation in a local hospital and

[46] http://www.retesan.ch

be presented online to specialists at a physically distant university hospital for diagnosis.

10.3 Social and economic developments

So far electronic health records (HER) and telemedicine are seen as promising tools for health care professionals, enabling them to provide better, safer and more efficient treatments for patients. But these developments will have wider implications: they will affect the relationship between patient and doctor, as well as work sharing and organisation in hospitals and primary sector. There are also privacy implications for both patient and medical professional. .

10.3.1 Trust

The TA-SWISS study on computer based patient's records (Patients' records [TA-SWISS 2000]) mentioned that their uptake might result in the patients losing trust in health professionals, because they might feel that their privacy has been compromised. The Danish citizen's panel (Electronic Health Record [DBT 2002]) also paid considerable attention to safety, protection of patient's rights and personal integrity, their positions on these issues being more clearly marked than with the paper health record. Similarly, the TA-SWISS telemedicine study (Telemedicine [TA-SWISS 2004]) notes that patients and health professionals confronted with e-Health become more aware about the meaning of privacy.

10.3.2 Empowerment versus responsibility

One of the often-cited advantages of e-Health is the empowerment of the patient: The patient is no longer a passive recipient of care, but can play an active part and influence his/her own treatment and care. This vision was shared both by the Danish citizen's panel and by the authors of the TA-SWISS study on telemedicine. However, the TA-SWISS study on computer based patient's records points out that the benefits of empowerment need to be measured against potential drawbacks arising from transfer of responsibility for data protection from public health organizations and/or medical doctors to the patient (particularly in the case of chips or cards detained by the patient) (Patients' records [TA-SWISS 2000]). The Danish Citizens panel also highlighted some drawbacks: for example, the right "not to know" - not all patients want all the information related to their diagnosis. They said that information about serious or terminal illness should be given face-to-face before the information is accessible in the EHR (Electronic Health Record [DBT 2002]).

The protection of privacy is not only relevant for the patient, but also for health professionals: the introduction of e-Health could lead to them being, or having the impression of being, continuously under control.

10.3.3 Access and data management

The protection of electronically stored health data is important for citizens, as shown by the results of the Danish citizen's conference (Electronic Health Record [DBT 2002]). According to them, the patient's approval of access is required in all non-acute situations. Moreover, only professionals involved in the care process should be granted access to the EHR. Each individual should have the possibility to grant extended access to the EHR. The citizens approved that data in EHR is used for research and statistics, but it should be rendered anonymous. And they argue for a code of ethics and discipline in the use of EHR data in research.

Similar conclusions are also made in the TA-SWISS study on telemedicine (Telemedecine [TA-SWISS 2004]), which insists that the patient should have the right to access his or her data and should decide who can access his/her data; in addition, any access to data should leave a trace and any change made should be digitally signed. The study on electronic patient records (Patient's Records [TA-SWISS 2000]) also highlighted the freedom for patients to decide to whom they want to pass on their data. Authors of the study insisted that this right should not be challenged by programmes or practices encouraging patients to give up voluntarily their medical data in exchange of some advantages (e.g. to get bonuses from the health insurance or to get a job)

Even though the development of ICT in all spheres of our lives raises concerns over data protection, there are also many potential benefits with respect to privacy. For example, increased privacy awareness amongst patients and health professionals could lead to a better application of data protection policy. The problems posed by privacy protection are handled more systematically in the context of telemedicine than some other areas, and the techniques might allow better data protection than before (Telemedicine [TA-SWISS 2004]).

However, both TA-SWISS studies on telemedicine and Electronic patients' records point out a number of potential threats to data protection: for example large amounts of data could be accessed or manipulated anonymously and from remote locations, without leaving a trace. Or data could be transmitted to countries with less rigid legislation on data protection. Data could potentially be accessed by other parties with a vested interest, not necessarily for the benefit of the patient, for example from insurers, employers, family, the media, the authorities, etc. All these concerns are related to access and ownership of the data, and the type of system that should be used.

Questions related to data protection as well as to ownership of the data are also raised by *biobanks*. Biobanks allow for storage of samples of human bodily substances (e.g. cells, tissue, blood, or DNA) that are or can be associated with personal data and information on their donors. In this respect, they constitute an important resource for identifying the causes and mechanisms of a large number of

diseases. To be able to investigate the complex interactions, it is necessary to gather large quantities of genetic and lifestyle data. These will be used to examine genetic factors, a central element of genome-based therapies. Biobanks and data protection have been addressed in a TA-SWISS study on pharmacogenetics and pharmaco-genomics[47].The authors of this study have identified a need for statutory regulation, and recommend strict data protection law provisions and as far as possible decentralised forms of organisation and pseudonymisation of samples. According to them, concomitant research should subsequently consider the ethical, legal and social aspects of biobanks, and there should be greater data security in the academic sector. From the point of view of insurances, symmetrical information between the insured and the insurers is crucial for adequate tariffs of risks.

10.3.4 Security as a priority

There is always the risk with e-health that important data concerning the patient are no longer accessible or are changed, for example owing to technical failure, or that access is gained to confidential information by unauthorised people. Today, little attention is often paid to the protection of patient data from such security threats. Awareness of this issue needs to be generally promoted in the health sector.

10.3.5 Public debate and Information

The citizens from the Danish panel did express a wish for more public debate on the issue of electronic health records (Electronic Health Record [DBT 2002]). In Switzerland, the study on telemedicine estimates that although up to now, telemedicine has been almost exclusively the preserve of specialists, because every person will sooner or later be a patient who will come into contact with telemedicine and computer based patients' records, they should be informed at an early stage about this new development (Telemedecine [TA-SWISS 2004]). Similarly, the authors of the electronic patients' records study called for a social debate via the media and public encounters (Patient's Records [TA-SWISS 2000]).

10.4 Economic issues

E-health is often presented as having major potential economic benefits for the health care system and for patients. Personnel resources can be employed in a more targeted way than previous, unnecessary waiting times and patient journeys can be avoided through telemedicine, etc. Costs can also be saved in cases where telemedicine supports the care of chronically sick or elderly people at home. The participants in the viWTA project on elderly and ICT saw the possibility of reducing health care costs while being able to stay longer at home, as a very attractive

[47] TA-SWISS: Pharmacogenetik und Pharmacogenomik, 2005 (http://www.ta-swiss.ch/www-remain/projects_archive/life_sciences/pharmacogenomics_e.htm).

advantage of telemedicine (Colourful Flanders [viWTA 2004]). With respect to EHR, many types of economic benefits are also expected. Among these, we can mention the possibility to avoid redundant examinations, more quality and efficiency in medical care and better epidemiological studies.

However, the TA-SWISS studies on electronic patient records and on telemedicine pointed out that these benefits might conflict with the protection of patients' privacy and that data protection measures can be costly in terms of material investments and training of health professionals (Telemedicine [TA-SWISS 2004], Patients' records [TA-SWISS 2000]). Moreover, they highlighted that investigations on the economic viability of e-health are generally conducted by institutions and persons that are themselves active in the field, and therefore have an interest in presenting the positive effects of this technological trend.

10.4.1 Research

The large amount of data gathered in the Electronic health records could be of great use for research and epidemiological studies leading potentially to a benefit for the entire population. The study on Computer based patient's records from TA-SWISS points at a possible trade-off between research for the collective good and the individual right for data protection (Patient's Records [TA-SWISS 2000]). The Danish citizen's from the Danish Board of Technology project approved that data in Electronic health records being used for research and statistics, because of the benefit for society. They did however insist on these data being made anonymous, as did the participants of the Swiss citizen's conference on research involving human beings discussed previously. Additionally, the citizens from the Danish panel wanted a code of ethics and discipline in the use of Electronic health records data in research (Electronic Health Record [DBT 2002]).

10.5 Political and legislative developments

10.5.1 Maintaining and reinforcing existing privacy rules

Privacy issues with respect to the health sector are particularly sensitive. Most European countries have relevant legislation, which guarantee data protection and data safety of patients. These, must certainly be maintained, if not reinforced. In Denmark, the citizens who participated in the consensus conference (Electronic Health Record [DBT 2002]) mentioned that existing legislation concerning patients' legal status and protection of personal data (privacy rights) should be respected, and that he rules for informed consent and the legislation for protection of patient rights and for protection of the individual in registry should be maintained as they are. The right for informed consent was also brought forward in the Norwegian Consensus Conference on the use of ICT to aid Elderly or Demented People in a humane manner (ICTs and the Elderly [NBT 2000]) and in the viWTA project on elderly and ICT (Colourful Flanders [vIWTA 2004]). In the latter project, the participants, all elderly

people (50 and more), stressed explicitly that e-health applications always need to take into account the privacy rights of patients.

It is also important that health sector players such as hospitals develop some particular recommendations with respect to data protection. Harmonization is also an issue, especially with respect to increasing internationalisation. The TA-SWISS studies also call for harmonization, as they have been done in the context of a federal country where a number of overlapping regulations and laws can be found at national and cantonal levels. Harmonization is also an important feature.

10.5.2 Privacy versus security and efficiency

The TA-SWISS studies (Patients' records [TA-SWISS 2000], Telemedicine [TA-SWISS 2004]), highlighted some tensions with respect to privacy and data protection. First, to which extent can patients hide information on their health which might also concern or put in danger their relatives or other persons (for instance information about an infectious disease)? There is a need to define which data are relevant in evaluating risk and how such data should be treated.

Second, how to assure both the privacy rights of patients and the efficiency of the health care system? As a matter of fact, guaranteeing patients data protection might be in contradiction with rapid data exchange for treatment or with large scale research and prevention activities. The experts in the viWTA study on elderly and ICT also stated that excessive privacy precautions might reduce one of the most attractive advantages of e-health applications, namely a very quick and reliable way of medical data exchange.

Third, overcomplicated security measures could lead to a two tier medical system, in which only the patients able to deal with the technologies can profit from them (Patients' records [TA-SWISS 2000], Telemedicine [TA-SWISS 2004]). Complicated measures might also be unwelcome by health professionals, as was also pointed out at the Danish citizen's conference.

10.5.3 Systems design

The Swiss and Danish projects (Patients' records [TA-SWISS 2000], Electronic Health Record [DBT 2002]) also looked at how the data would be stored. Both projects showed that patients were more in favour of a card system than a virtual dossier, and the TA-SWISS study showed that chip implementation idea was not acceptable. However, decisions would need to be made on who would be able to deliver the cards, make security copies and perform security tests – this responsibility could either lie with the authorities or with an accredited organisation. Whether to choose a centralised or a decentralised approach to developing the nation-wide EHR system has to do with challenges such as securing interoperability and maintaining flexibility in ICT-system suppliers.

10.6 Concluding remarks

The use of ICT in healthcare gives raise to concern and poses crucial questions about privacy as it deals with information, which most people find very sensitive. Therefore, privacy should be carefully considered in this area.

The implementation of e.g. Electronic Health Records does not merely provide an (expected) increased efficiency among health care professionals. e-Health does potentially change the relation between patient and doctor, the work flows and organization in hospitals, and it is likely that it involves increased data exchange. This gives raise to a number of questions about ownership and control of data.

The patient's confidence in the doctor and the health system is crucial, and this should be an important consideration in the design of e-Health solutions - which should on the one hand ensure privacy for the individual, but at the same time find ways to benefit the "collective good", e.g. the potentials of using data for statistics in research in tracing trends in treatment etc. Moreover, it could be highly relevant to involve citizens and hospital staff in the design process.

ICT in healthcare can be implemented on the expense of the individual's right to privacy, but the technology can also be used to strengthen privacy, e.g. by implementing a real informed consent by technical means. Also, there are technical solutions to ensure that data from the health sector can be used for research purpose in a way that ensures anonymity. Which solutions one prefers is largely a political decision, and a decision with far reaching implications.

Chapter 11 Conclusions and policy options

Privacy is a fundamental right and an important societal value. Technological developments make it practically impossible for individuals to participate in modern society without leaving electronic traces – and thus compromising their privacy. This report has focused on the trade-offs that have to be made in order to function in modern society.

Dealing with privacy in terms of trade-offs helps illustrate that a balance has to be found between conflicting societal values and rights. In this report we have introduced five important areas that affect privacy: Security, access to information and services, societal interaction, convenience and economic benefit. How individuals choose to deal with these areas in terms of trading off some of their privacy is often a matter of choice, but it is also affected by public policies and legislation.

11.1 Why we need a renewed policy on privacy

The balance between the areas mentioned above and privacy seems to be increasingly challenged:

We are leaving traces – and systems don't forget
ICTs are constantly developing, extending the possibilities for data collection, storage and analysis. Wherever you go, you leave "electronic footprints" that can easily be stored, copied and search through for an indefinite period of time. Developments in the IT sector over the last years have made possible huge collections of data, be they for medical purposes, security concerns or just to allow the delivery of certain services. Furthermore, pervasive computing may lead to the collection of huge amounts of data on individuals without their knowledge.

Because so many of the technologies used in everyday life may affect our privacy, it has for all practical purposes become impossible for individuals to keep track of all traces they leave and to take precautions against it.

Short term gains but long-term effects
A lot of services generally perceived as beneficial, like e-Health or e-Government registers, require the collection of large amounts of data. Anti-terror policy is an example of a service which to a certain extent takes advantage of the technological advances made in person recognition, location and communication.

But this is not the only driving force towards a so-called "surveillance society". The drive for efficiency also constitutes a major force towards more data collections and analysis: Rationalisation in health leads to electronic health records, rationalisation in commerce leads to individual advertisement (customer relationship management) or

on-demand production and rationalisation in public administration may lead to different means of electronic identification and an increase in data exchange between units.

An unbalanced relationship

Although privacy is highly appreciated in legal terms there seems to be little awareness of it among users, politicians and economical actors. However, limited awareness doesn't mean ignorance. Many users know that they give away information, but they can't be expected to have an overview of the long-term and cumulative consequences and implications. There is a great divide between the individuals and the professional parties in knowledge about possible usage and economical value of personal data.

Even users that are aware of privacy issues find it too inconvenient to deal with them. Because of the complexity of new systems, the asymmetry of knowledge and the need for privacy, the government has a responsibility to strengthen the privacy culture and to ensure proper system design. This cannot be done by the end-users, but by professional parties, such as businesses or public authorities.

The need for a precautionary approach

The development of ICT is in many ways an irreversible phenomenon. This means that poorly designed ICT products today may affect privacy in 10 or 20 years time. Adopting a precautionary approach, however, does not mean stopping the development of ICT – it implies finding a balance.

A sound balance implies a precautionary approach from users, developers and policy-makers, which reduces privacy risks to a minimum. This report gives a list of options that should be considered by policy makers.

One step to adopt the precautionary principle may be to create awareness and a social dialogue on the impacts of widespread use of ICT or pervasive computing. Raising awareness of privacy among the public is not only a matter of providing information, it is equally important to initiate a wide social debate on privacy: what is perceived as violating citizens' integrity, and what is not? This can happen through conferences, public consultations or cultural events. Moreover, privacy should be discussed based on specific issues, such as RFID technology, e-government or biometrics.

11.2 The challenges – and how to deal with them

Often, when discussing privacy issues, the considerations and proposed solutions concentrate on one dimension. Discussions often take part in limited circles: lawyers discuss on their side and technologists on theirs. Technology assessment offers a horizontal approach, in which legal, technical and social solutions have to be coordinated and consequently implemented. This calls for an active role for policy-makers.

The following sections list seven challenges related to privacy, and the policy options that should be considered in response to these challenges.

Challenge #1: To provide security without infringing privacy

Governments try to provide their citizens with a high level of security. But the drive for improved security is often attributed to an ulterior motive of increasing surveillance. As a general rule, the benefits of surveillance systems should be carefully considered and compared with alternatives.

In some cases surveillance systems or measures may be justified to promote security or public safety.

Implement surveillance systems only if they are effective, not easily circumvented, and will produce a real security benefit

The principle of proportionality states that surveillance systems should only be implemented if the benefits are worth the social costs, including the invasion of privacy, loss of autonomy, social discrimination, or imposition of conformity.

Assess surveillance systems at all stages

If the surveillance systems produce a security benefit that justifies the social costs, measures should be taken to minimise those costs. Before any surveillance system is implemented, legal mechanisms of oversight and redress will have to be established.

The effects – both positive and negative – of the systems should be periodically reviewed by an independent publicly accountable body.

Challenge # 2: e-government makes citizens more transparent to the authorities

The primary driving force for implementing e-Government is the need for rationalisation and efficiency in public administration and convenience for citizens. E-Government solutions are often designed to increase the flow of information between different public units, in order to provide the desired service. A vital challenge is how the technology can be used not only to increase efficiency for the public administration; but also to strengthen privacy for the citizen – and thus create mutual transparency.

Empower citizens to real informed consent

Technology can be employed to make it easier for the citizen to give their *voluntary, specific, and informed* consent for the disclosure of data. The exchange of data between various administrative agencies in e-Government might only occur upon a formal request for the disclosure of personal data.

Give citizen access to case records and logs

IT systems can be designed in a way that gives citizens direct access to their own records. The right to access can be more rigorously enforced and extended to a wider number of administrative areas. This will require changes in legislation.

Citizens may be given access to log files with information concerning who has created, seen, changed, forwarded, or received information regarding that citizen.

It is important to ensure record keeping and the accessibility of digital journals and data. Digitalisation increases the need for logging, as electronic documents are easily changed and original copies can be lost, etc.

Challenge # 3: The enforcement of privacy legislation is too weak

In many of the countries mentioned in this report, privacy regulation exists, but is not properly enforced. The mandate of data protection agencies remains weak. As long as ignoring data protection rules bears no consequence, there will be no incentive for industries and public bodies to incorporate privacy principles in their IT systems and services.

Strengthen the mandate of data protection agencies

Governments need to consider seriously whether data protection agencies should be able to conduct investigations, monitor activities of public and private organisations and their data systems approaches. At the very least, they should be enabled to handle complaints in due time and to state fines.

Without appropriate sanctions and penalties, there is less motivation for private or public organisations to develop and implement privacy-compatible IT systems, especially if such systems imply more costs for them. Privacy legislation can be updated to incorporate enforcement measures, which dissuade private and public institutions from ignoring data protection rules.

Data protection agencies could also have a role in delivering privacy labels. Labels are an important feature to guarantee trust from the users, as they prove that the system is compatible with privacy standards (see below). The idea would be to have common labels which are known by the public and that are delivered by a competent, trusted and neutral institution.

Data protection agencies may well act as a focal point, for citizens to ask for information, indicate suspicious cases or address their complaint.

Allocate more resources to data protection agencies

Parallel to the strengthening of their mandate, data protection agencies need enough resources in terms of finances and personnel in order to be able to fulfil their tasks.

Challenge #4: Systems development neglects privacy

Too often, privacy threats could be avoided if data protection concerns were integrated in information systems development from the beginning. This implies both legislative and technical adaptations.

Encourage data minimisation and privacy enhancing system designs
Privacy enhancing technologies (PETs) should be systematically integrated in systems development. Such technologies are not a panacea to solve all privacy issues, but they can significantly contribute to minimising data collection and analysis. An important PET principle is that systems should only collect data on a *need to know* – not *nice to know* – basis. Delivering services without collecting excess data should be encouraged.

Make privacy impact assessment mandatory
Privacy impact assessments (PIAs) should be encouraged when building and (re)designing technical systems. PIA is commonly based on the OECD code of fair information practices and aims to assure that all privacy issues have been identified and that personal information is being properly protected.

In the public sector, privacy impact assessments should become a prerequisite to procurements. Although PIA will claim human capital, the benefits may be significant. It is cheaper to include privacy concerns in the design phase of systems than to fix systems at a later stage to make them privacy compliant.

Contribute to international privacy standards
There is a need for international privacy standards. Such standards are a prerequisite for developing privacy-compliant IT systems. International privacy standards have many advantages: They enhance consumer trust and ensure equal privacy protection worldwide; and they encourage corporate responsibility.

National standard bodies, ISO, trade associations, relevant European and national ministries and data protection authorities should take part in the development of such standards.

Require the use of best available technologies (BAT)
Current regulation requires the use of best available technologies for data security but not for privacy. A legal obligation to implement state of the art technology for privacy protection could support privacy friendly systems design considerably.

Make privacy part of the funding criteria for ICT research
Publicly funded ICT research may serve as an example, and in this respect, only privacy-compliant projects should be funded. This would imply having privacy as one of the criteria for the ethical evaluation of ICT research. European research bodies, as well as national funding institutions, could carry this out.

Challenge #6: The value of privacy is underestimated

For companies the challenge is to uphold the balance between collecting information for marketing purposes and respecting their customers' privacy. This seems to be best done by not asking for information that is unnecessary for the service, and by upholding a strict privacy policy. The latter involves storing the data in a secure way, not using it for other purposes than stated in the privacy policy and not reselling the data to others.

However, little is done to incite industries or private bodies to implement privacies, be they with positive measures (e.g. labels) or sanctions.

Promote an unique European Privacy Label

As in many other domains, privacy labels could be used in order to incite industries or public entities to build and design privacy-compatible ICT systems. If a certain label is known and acknowledged by the users, products carrying this label might have a clear competitive advantage.

For a label to be known and acknowledged, it should be unique and awarded through a credible institution (for instance the national data protection agency). For the time being, no such label exists. A process to develop a privacy label should involve all key-actors (national standard bodies and ISO, trade associations, ministries, data protection authorities).

Challenge #7: To create privacy policies based on research

Effective regulation is based on knowledge. Many of the uncertainties about the mid- and long term effects of data collection and analysis are not known yet. Even the full potential of data retention applications is still not known. It can be assumed that ongoing and future developments in this area will have implications in many fields and that this will have impact on legislation. This calls for actions to be taken in order to understand the implications for privacy.

Explore the technological development and its legislative implications

There is a need for research aimed at better understanding the mid- and long-term effects of data collection, storage, processing and exchange. How will the technology develop? Will this development be compatible with current privacy legislation, or will it require a revision of current practices in data protection?

Initiate research on social consequences of increased data retention

When considering the effects of technological developments mentioned above, indirect consequences should also be considered. For instance, even though one's data are not systematically stored and analysed, the fact that technology makes it possible may lead people to behave as if they were under surveillance, and thus increase social conformity. How will social relationships be transformed by a

surveillance society? And how may this affect the individual's perception of his own identity?

Challenge #8: Future pervasive systems multiply the challenges to privacy

New technological challenges will bring new challenges for privacy. Pervasive computing is the vision of networked processors, communicating with each other to perform defined tasks. In order to function, such pervasive systems will require the collection of huge amounts of data on their environment. Pervasive systems thus accentuate the challenges to privacy, as they foresee the physical disappearance of computers – computers will be able to deliver services without being noticed and without human intervention.

Adapt regulation to the new reality

Existing regulations certainly need to be adapted in the direction of "System data protection". This implies that next to general principles outlined in current legislations (proportionality, information and purpose principle), the legislator defines processes for the development of IT systems. Such processes could, for instance, propose that the data protection agencies should be consulted in all cases, that the IT systems integrate functions that guarantee transparency for the users, that the communicating devices are clearly marked, etc.

Make pervasive systems visble

When possible, pervasive systems should be made visible. For instance, when entering a room with pervasive devices, a special sign could be displayed. Tagged objects should also be specially marked.

Establish ICT free zones

Privacy protected zones could be offered to those who don't want to be surveilled. As often as possible, opt-in solutions should be the default. When possible, users should be asked if they want to use context sensitive IT systems. "ICT free zones" where users have the possibility to retreat should be established.

Ensure Log-off/switch-off possibility

For many devices being part of a pervasive system, the on-line status is default. And very often, there is no alternative. New IT systems should offer off-line as the default status. If not possible – because the system cannot function off-line -, the system should in any case offer an easy and simple possibility for the users to switch-off.

Appendix A – Overview of Technologies

This appendix covers technical developments in ICTs that either threaten or enhance privacy.

Internet/networks

The past decade has seen vast expansion of the use of the internet. As a result of this, people leave digital “footprints” when they surf, shop online, talk on the phone, do their banking etc. In many cases the users are not aware of the extent of the traces they leave when they use ICTs in their everyday tasks. In addition to an increase in the amount of traces, we see that the traces contain more comprehensive information about the user and his/her actions. Examples include:

IP-address
An IP-address is an identifier for a computer or device on a Transmission Control Protocol (TCP) / Internet Protocol (IP) network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. Connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates. When a user visits a web-server, it will often store information about the user’s visit on its various web pages. This information will typically be time, the user’s IP-address, user-name for the internet account and which pages were visited. If the user has a fixed IP-address and is not using address mapping in a firewall, the user’s machine can be uniquely identified.

HTTP-references
The HyperText Transfer Protocol (HTTP) works so that when a link from one page to another is followed, the address (URL) from this page is sent with the request for the new page. The new site can then see which site the user came from, and in this way gather information about the user’s activities on the net. When clicking a link after a search, the words in the search sting will normally be part of the URL, and thus passed along to the new web site. This can be used to build a profile on the user. In many cases the search engine supplies ads from companies with ads on the pages listed as hits from a search. These ads are normally loaded straight from the advertising companies’ servers. This means that all these companies will receive information about the user’s search string.

Cookies
Cookies are messages given to a Web browser by a Web server. The browser stores the message in a text file on the user’s computer. The message is then sent back to the server each time the browser requests a page from the server that supplied it. The main purpose of cookies is to identify users and possibly prepare customized Web

pages for them. The server can use the information in the cookie to present custom Web pages.

Two different types of actors can store cookies on the user's computer. First party cookies are created by the web server visited by the user. Third party cookies, on the other hand, are created by companies advertising on the site visited. These cookies can be used for gathering information about the user's surfing habits on pages where the company advertise, and can be used for marketing purposes.

E-mail
E-mail are messages transmitted over communications networks. When a message is sent, it can be stored on two or more different servers on its way from sender to recipient. Unless it's encrypted, it can be read by people who have access to these servers. Apart from the content of the message, information about sender's and recipient's IP-address and which addresses the message had passed through on the way between them can be logged. Some countries monitor this information systematically, e.g. the USA.

Spam
Electronic junk mail or junk newsgroup postings, sometimes defined even more generally as any unsolicited e-mail. However, real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted e-mail. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. Some online services have instituted policies to prevent spammers from spamming their subscribers.

Phishing
Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Website, however, is bogus and set up only to steal the user's information.

Adware
Adware or advertising-supported software is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used. Adware often comes "bundled" with spyware.

Spyware

Spyware is the term used for any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Local data

History

The history of activity on the Internet can be stored locally for easy re-access. This makes it possible for other users of the computer to see what sites have been visited.

Cache

Pronounced *cash.* Cache is a special high-speed storage mechanism. The content of the cache can be viewed directly by other users on the same computer. On a private computer this may not be a big problem, but on a communal computer, for instance in a library or internet café, sensitive information, like forms the user had filled in with personal information, could be made available to strangers.

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. A Firewall will log all incoming and outgoing traffic. Using tools that come with the firewall, system administrators or other with the appropriate access rights can see who has visited which web sites, how many times and for how long. This technology enables en employer to monitor the employees' use of the internet extensively.

DRM (Digital Rights Management)

This technology is meant to ensure the legal rights to digital content such as music, movies and text. Most of the solutions that exist today require that the user identifies to prove that he or she has the right to access the content. This limits the access to anonymous use, and makes it possible to build profiles with information about the users taste in entertainment.

Mobile services

Communications data

Exchanging information using ICTs can provide data which falls into three categories:

- *Traffic data*: who exchanged information, when, how long for? The digitalisation of fixed networks reversed the situation regarding traffic data, because data which was previously very difficult to obtain was now easily available, creating the need to establish rules for deleting it.
- *Location data*: this is data on where the involved parties were at the time they had contact. Mobile services are now adding location information (with the advent of 3G networks). Some countries that require mobile phones to have this functionality for the purpose of locating callers in emergencies (the USA, Japan from 2007).
- *Content*: what information was exchanged

Location based services

Location based services calculate the position of the user's mobile equipment by using known coordinates of for instance GSM base stations.

The calculations give an approximate position that can vary from a few hundred metres in densely populated areas to several kilometres in rural areas. The accuracy can be enhanced by taking the signal delay into consideration. More accurate methods are "Enhanced time difference (for GSM) or "Observed time difference of arrival" (For UMTS). These methods take advantage of the fact that users normally are within range of several base stations at once and use the relative delays to the different base stations to calculate the position, normally within 100-300 metres.

The same principles can be used with other types of base stations, such as WLAN or Bluetooth. These technologies have a shorter range, and the accuracy will therefore be higher.

GPRS/UMTS

These technologies are based on packet-switching. This means that the user in effect is always logged on, and pays only for the amount of data transferred. It is assumed that this technology will lead to an increase in location based services.

Bluetooth

A short-range radio technology aimed at simplifying communications among Internet devices and between devices and the Internet. It also aims to simplify data synchronization between Internet devices and other computers.

WLAN
Acronym for *wireless local-area network*, also referred to as *WLAN*. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

GPS
Short for *Global Positioning System*, a worldwide satellite navigational system formed by 24 satellites orbiting the earth and their corresponding receivers on the earth. Each GPS satellite continuously transmits digital radio signals that contain data on the satellite's location and the exact time to the earth-bound receivers. The satellites are equipped with atomic clocks that are precise to within a billionth of a second. Based on this information the receivers know how long it takes for the signal to reach the receiver on earth. As each signal travels at the speed of light, the longer it takes the receiver to get the signal, the farther away the satellite is. By knowing how far away a satellite is, the receiver knows that it is located somewhere on the surface of an imaginary sphere centred at the satellite. By using three satellites, GPS can calculate the longitude and latitude of the receiver based on where the three spheres intersect. By using four satellites, GPS can also determine altitude.

Surveillance technologies

CCTV
Public and private CCTV schemes can be deployed for a number of reasons:

- *Monitoring public areas* to detect incidents and to coordinate police responses.
- *Recording events* for use as evidence and to inform investigations. For instance, on the boundaries of the Parliamentary estate, police on patrol alert CCTV operators of incidents via radio links. CCTV operators then record incidents as they unfold.
- *Directed surveillance* of suspected offenders.
- *Deterrence* of criminal activity – although the evidence for this is inconclusive.

Information management
CCTV control rooms may deal with information from many cameras. 'Smart' technologies can alert operators to pre-determined people, registration numbers or incidents, reducing the need for CCTV to be constantly monitored However the effectiveness of these systems depends upon the reference information (e.g. licence plate databases) being accurate and up to date.

Echelon
The Echelon network is run by an alliance of the USA, UK, Canada, Australia and New Zealand. The system has been in operation since the cold war, and was initially set up to monitor communication in or to the Soviet Union and Eastern Europe.

The system's purpose is to monitor private and commercial communication – which means non-military communication. It is stated that the system can perform quasi-total surveillance, which means that all types of electronic communication – telephone conversations, SMS, fax, e-mail and internet traffic – can be monitored. Patterns of communication can be analysed, and content can be scanned for interesting keywords. Messages that are identified by the system are copied for manual evaluation.

Even though the system can capture a significant part of satellite- and radio based communication, it has only limited access to communication via cable.

Small memory technologies

RFID

RFID tags are seen as the next generation of 'bar codes' However, unlike bar codes, which can only be used to identify a *type* of product, RFID tags can store a large amount of information and could therefore be used to uniquely identify a product ("item level tagging") or to store personal data. Previously tags were only used in closed systems – e.g. within the supply chain of individual retail companies. However, as the cost of tags decreases and worldwide industry accepted standards become available, item level tagging is becoming more widespread.

The main privacy concerns regarding RFID tags are related to the following:

- use of data by a third party
- an increase in direct marketing
- the ability to track individuals

Smart cards, chip cards.

A smart card is a small electronic device about the size of a credit card that contains electronic memory, and an embedded integrated circuit (IC). Smart cards are used for a variety of purposes, including:

- Storing a patient's medical records
- Storing digital cash
- Generating network identifications.

A smart card will also contain some means of identifying an individual, and can be used to provide them with access to public or private services.

Data mining

Data mining is a label for technologies which find useful patterns and rules within large amount of data. As an indirect consequence these technologies foster the creation of

large data pools (data warehouses) which could not have been analysed effectively with traditional methods.

A simple example of data mining is its use in a retail sales department. If a store tracks the purchases of a customer and notices that a customer buys a lot of silk shirts, the data mining system will make a correlation between that customer and silk shirts. The sales department will look at that information and may begin direct mail marketing of silk shirts to that customer, or it may alternatively attempt to get the customer to buy a wider range of products. In this case, the data mining system used by the retail store discovered new information about the customer that was previously unknown to the company. Another widely used (though hypothetical) example is that of a very large North American chain of supermarkets. Through intensive analysis of the transactions and the goods bought over a period of time, analysts found that beers and diapers were often bought together. Though explaining this interrelation might be difficult, taking advantage of it, on the other hand, should not be hard (e.g. placing the high-profit diapers next to the high-profit beers). This technique is often referred to as "Market Basket Analysis".

Identity and Identification

Privacy in the information age is closely related to the concept of identity. To be able to hold individuals responsible for their actions, there's a need to be able to identify the person responsible. To protect people's privacy, on the other hand, it's necessary to protect them against unnecessary identification. The balance between these two considerations is one of the big dilemmas in the information society, and how these considerations are made are of great importance for privacy. To a certain degree, electronic communication can handle both these considerations by allowing use of different forms of digital identities.

Digital and virtual identities

Digital identity is an electronic representation of identity, that is a collection of identifying information in electronic form. All identification on the internet is based on the use of digital identities. This concept is very broad, and involves everything from procedural identity in digital form (that can identify a physical person) to virtual identities that have a very weak connection to a physical person.

Virtual identities (also known as *nym*) are a form of digital identity. These electronic identities express a bigger or smaller set of an individual's personal information. These types of identities can be used to weaken the connection between electronic traces and an actual person, and reduce the danger of someone aggregating personal information in a profile. As such virtual identities are essential tools to ensure privacy in the information age.

Anonymity and pseudonymity
What degree of identification can be connected to the electronic traces is the key to how electronic traces affect privacy. Of the essence is whether the traces can be connected to a physical person and how easily this can be done. If it's easy to connect electronic traces or data to an individual (i.e. if a phone number or social security number is connected to the data) it can be considered a privacy problem.

Authentication
Identification is about finding out who somebody is. This involves finding an answer to the question: "Who are you?" Authentication is closely linked to identification, as it deals with the verification of identity. Authentication is about finding the answer to the question "Are you who you say you are?"

Authentication is normally done for one out of two reasons. In some cases it's about restricting access to services or information, or the protection of resources. The other reason is a need to authenticate users to be able to hold them responsible for their actions.

More and more services use systems for authentication to give users access. E-commerce and e-government are important drivers for increasingly sophisticated systems for authentication. There are several technologies for this purpose, and even though it's rarely necessary, almost all systems use personal information in the process. This gives us reason to be concerned about privacy.

Authentication is a complex issue, closely related to both security and privacy. We can look at authentication on three levels:

- *Authentication of an individual*
  This establishes to a certain degree that an identifier refers to a specific individual, a physical person.
- *Authentication of an identity*
  This establishes to a certain degree that an identifier refers to a given identity (often virtual). It can be possible to link this identity to a physical person, but it doesn't have to be.
- *Authentication of an attribute*
  This establishes to a certain degree that an attribute or quality is connected to a given user, for example that the user is of a certain age (i.e. over 18).

Both whether one chooses to authenticate and what type of authentication one chooses for a certain service, is of great importance for privacy. It's therefore important that the degree of authentication is fitting to the purpose, and that not stronger or more invading methods than necessary are used.

Three different characteristics are normally used to authenticate someone's identity:

- Something they know (i.e. a password or PIN-code)
- Something they have (i.e. ID, smart-card or other type of identification)
- Something they are (physical characteristics, biometrics)

Passwords
A password is a secret series of characters that enables a user to access a file, computer, or program. On multi-user systems, each user must enter his or her password before the computer will respond to commands. The password helps ensure that unauthorized users do not access the computer. In addition, data files and programs may require a password. Ideally, the password should be something that nobody could guess. In practice, most people choose a password that is easy to remember, such as their name or their initials. This is one reason it is relatively easy to break into most computer systems.

Biometrics
Biometric technology identifies individuals automatically by using their biological or behavioural characteristics. The most common biometric is automated fingerprinting - the analysis of an individual's unique fingerprints - but emerging technologies include:

- *face*: the analysis of facial characteristics
- *hand geometry*: the analysis of the shape of the hand and the length of the fingers
- *retina*: the analysis of the capillary vessels located at the back of the eye
- *iris*: the analysis of the coloured ring that surrounds the eye's pupil
- *signature*: the analysis of the way a person signs his/her name.
- *vein*: the analysis of pattern of veins in the back if the hand and the wrist
- *voice*: the analysis of the tone, pitch, cadence and frequency of a person's voice.

Ubiquitous computing

Ubiquitous computing (also referred to as pervasive computing or ambient intelligence) integrates computation into the environment, rather than having computers which are distinct objects. Promoters of this idea hope that embedding computation into the environment would enable people to move around and interact with computers more naturally than they currently do. One of the goals of ubiquitous computing is to enable devices to sense changes in their environment and to

automatically adapt and act based on these changes based on user needs and preferences.

Privacy Enhancing Technologies

Technical progress does, of course, also offer new opportunities to protect one's privacy through technology. The cryptographic foundations for anonymous Internet use were developed already at the beginning of the eighties. These concepts were further developed and attempts undertaken to transform them into services and software once the Internet started to expand. In the middle of the nineties the term "PETs - Privacy Enhancing Technologies" was established for this field of technology.

PETs have been defined as a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system.

Encryption

It is important that sensitive information is sent and stored in encrypted format. Many 3rd parties have access to e-mail messages or documents stored on various servers. The privacy of an un-encrypted e-mail message can be compared to that of a postcard. Encryption can, on the other hand, be compared to putting the content into a virtually unbreakable envelope. Using modern strong encryption, the message will in the foreseeable future be secure against opening without the recipient's key.

Appendix B – Methods

Citizens' panels

This method is based on the model of Consensus Conferences, but does not require the same amount of time and effort from the parties involved.

The citizens' panel consists typically of 14-18 citizens that only represent themselves. They do not have to have prior knowledge of the topic in question. The participants are recruited through ads in the national and local press (depending on what is relevant to the topic) and letters to a random selection within the relevant demographic group. The group should be as heterogeneous as possible. The idea is that a group of ordinary citizens (lay people) given sufficient information on a difficult and complex topic can take a holistic view to the best of society.

The group meets 3-4 times and works on a statement that will be delivered to the relevant authorities at the end of the process. The group decides for themselves whether to give general advice or detailed suggestions.

The meetings should not be too far apart, but one should allow for time to book experts and make changes in the agenda at the request of the panel. During the meetings the group gets information on the topic, and they can ask to get more information on issues they feel are unclear.

Consensus Conference

The consensus conference is a method, which involves citizens and gives them the central role in technology assessment. The citizens do not have any specific knowledge or relationship to the subject of the conference, and therefore act as laypersons that contribute by expressing their visions, concerns, values and experiences from their everyday life. The idea of the method is to enrich and expand the scope of a debate.

New technologies and scientific achievements often pose ethical dilemmas and uncertainties regarding possible long-time effects, which can leave decisions-makers perplexed. This goes for a number of technologies, such as stem cells research, genetic modified crops, as well as privacy issues in relation to ICT. As science and technology is becoming still more pervasive and as society is increasingly dependent upon and build around technology it is important to ensure political influence over science and technology. If only experts such as scientists and engineers deal with technology, and if citizens are in general excluded from the early stages of innovation, society will potentially face democratic deficit and technology can appear as determining or controlling society, rather than supporting a wanted development. This can give raise to political controversies at a time when it is too late to make any

significant changes. But if we can succeed in involving laypersons in technology assessment it might be possible to reach *robust* political decisions about technology; decisions which find support in the general public and therefore can be a part of a long time strategy.

The point of departure in the Consensus Conference - and other participatory methods in technology assessment - is that technology is socially constructed, and therefore cannot be assessed solely on a rational and scientific basis. There exist many competing interpretations of a given technology, and with the consensus conference, citizens are given the leading role in the assessment process by contributing with perspectives beyond scientific knowledge. The citizens are layperson in relation to the subject discussed, and they are recruited in a way that ensures a mix of gender, age, occupation etc. The 14 – 16 chosen citizens contribute with their personal point of view in terms of visions, worries, and experiences from their everyday life. Through 2- 3 weekends they enter a dialogue with each other, and in the process they formulate questions to a panel of experts. By the end of the process they reach consensus and formulate their recommendations for politicians and stakeholders.

The Danish Board of Technology developed the Consensus Conference in mid 1980's, and the method has been applied in different countries, e.g. the UK, France, Norway, Canada and Japan.

More about the Consensus Conference:
http://www.tekno.dk/subpage.php3?article=468&toppic=kategori12&language=uk

Desktop research

Desktop research involves drawing on existing literature as well as conducting interviews with key stakeholders, and then summarising the results in a written report. This can be a useful way of summarising the state of knowledge of a given subject and providing an overview of current debate surrounding it.

Stakeholders would be normally be consulted from a range of interest groups, including government, industry, NGOs, consumer groups and academia. Interviews can take place face to face, or over the telephone, or even e-mail. The same stakeholders can then be called upon to review the draft report and confirm that their views have been accurately represented. The scope of the literature review and the number of stakeholders consulted depend on scope and the intended length of the final report. The internet is a crucial tool for conducting the literature review and even for identifying stakeholders and experts on a subject.

"POSTnotes" published by the Parliamentary Office of Science and Technology and cited in this report, are produced by means of desktop research. They are four page

briefing notes aimed at providing UK Parliamentarians with an objective overview of a scientific or technological issue with a basis in public policy. They are normally structured to include a short technological background section, followed by a discussion of policy issues. Production of a POSTnote normally takes 3 months: roughly one month for literature reviews and interviews, one month for drafting, and one month for review of the POSTnote by external experts.

Such methods are a useful means of providing non-experts with a synopsis of a complex issue and enabling them to interpret the vast quantities of information on the subject from other sources, such as the media, NGOs and government, which they might encounter on a daily basis. The advantage of this method is that the process itself is not time consuming. Much of the literature review can be conducted over the internet. Also, interviewees and reviewers do not necessarily have to meet the researcher “face to face”. This means that such projects can solicit input from a range of international experts.

Expert panel / work group

The main task of an expert panel/work group is usually to synthesize a variety of inputs – testimony, research reports, outputs of forecasting methods etc – and produce a report that provides a vision and/or recommendations for future possibilities and needs for the topics under analysis.

The expert panel/work group often takes professional stock of the situation and proposes possible courses of action to ensure, initiate, promote or check development in the area. The purpose is often to provide a factual overview of a given area and make recommendations for further action. These recommendations are often directed at MPs, councils and municipalities, but other stakeholders and decision-makers may also be the target of the group’s work.

Expert panels are particularly appropriate for issues that require specialist knowledge, issues that are highly complex and require the synthesis for experts from many different disciplines. The method is not designed for and rarely involves the broad public directly.

Specific tools may be employed to select and motivate the experts, assign tasks and elicit sharing and further development of knowledge.

The panel or work group may consist of 5-8 specialists appointed by the TA-Institution. Members are personally selected and thus do not represent their respective institutions or organizations. To ensure an inter-disciplinarity group or panel members are appointed on the basis of different technical approaches, knowledge and networks.

If you want to read more about the expert panel method:
http://www.kbs-frb.be/files/db/EN/PUB_1540_Toolkit_7_ExpertPanel.pdf

And about the work group method:
http://www.tekno.dk/subpage.php3?article=467&toppic=kategori12&language=uk

Focus group studies

A focus group study resembles a structured group interview, where 7-10 persons with special knowledge or background discuss a topic with the interviewer. A typical focus group can be “young users of mobile services”, “master degree students in marine technology” or “parents of children with allergies”. The participants are qualified through their personal experiences as technology users, students or parents. The demographics of a group will vary with the topic in question. A group of master degree students will naturally be quite homogenous where age is concerned, while a group discussing the eating habits of Norwegians can be heterogeneous in age, sex, geography etc.

The topic of a focus group study is defined by the interviewer. Despite this it’s important that the discussions are sufficiently open to allow for the participants to exchange experiences and comments on each other’s viewpoints. Herein lies some of the strength of this method: Through conversation and group interaction you get more information than you would if you interviewed each member of the group separately.

A focus group normally meets 1-2 times. As a rule a subject is discussed until the participants start repeating themselves and no new information comes up. A meeting normally lasts 2-3 hours.

The method is particularly good when you want information about participants’ attitudes and norms. This could be young users’ thoughts on the dangers of leaving electronic traces or students’ expectations of a future in marine technology.

A focus group has a limited number of participants, and the results can of course not be generalised and be used as representative for a population.

Appendix C – Overview of Projects

This report is based on a series of projects conducted by EPTA members in six European counties. This appendix gives more information about each of these projects, including a brief summary and links to the full reports. The projects are listed alphabetically on short name.

Attitudes to Privacy [NBT 2004]	**Attitudes to Privacy – Focus Group Study on Electronic Traces and Privacy**	The Norwegian Board of Technology	2004
Content	For the focus group study 6 groups were put together, with 8 persons in each group. 4 groups covered the age group 17-19 years, and 2 groups consisted of people in the age 30-40 years. Different subjects related to privacy were discussed, and the results were published in a report called “Attitudes towards Privacy” in February 2004		
Original language:	Norwegian		
English summary			
Further information	http://www.teknologiradet.no/Rapport_fokusgrupper_9-5lz.pdf.file		

Biometrics [POST 2001]	**Biometrics and Security**	Parliamentary Office of Science and Technology	2001
Content	This briefing provided a technical overview of different biometric systems, with potential applications in criminal justice system and counter terrorist activities, and examined evidence on system performance and reliability. It was written to give Parliamentarians the opportunity to discuss issues relating to the use of biometric technology in prior to the introduction of the emergency anti-terrorism bill.		
Original language:	English		
English summary	http://www.parliament.uk/parliamentary_offices/post/biology.cfm#2001		
Further information	http://www.parliament.uk/post		

Biometric Passports [NBT 2005]	**Biometric Information Stored Electronically in Passports**	The Norwegian Board of Technology	2005
Content	As a response to demands from the USA, Norway started producing passports where biometric information (picture) is stored electronically from October 1st 2005. The police authorities have also proposed that fingerprints (in accordance with EU's proposals) should be stored in Norwegian passports in the future. In addition, the proposal suggests that the biometric information in the passport also should be stored in a central database. The reason given is that this will make it easier to produce new passports in case of stolen or lost passports (although it is also stated that the stored fingerprint information should be stored in a format that makes it impossible to reproduce the original fingerprint). It is also suggested that it should be possible for other (commercial) actors that issue identity cards to verify identity against the central passport database in exchange for a fee.		
Original language:	Norwegian		
English summary			
Further information	http://www.teknologiradet.no/files/hringsuttalelse_biometrisk_pass.pdf		

CCTV [POST 2002]	**Closed Circuit Television (CCTV)**	Parliamentary Office of Science and Technology	2002
Content	This briefing examined the effectiveness of CCTV schemes in England and Wales. It describes how CCTV is used and examines issues such as its effectiveness, civil liberties and its use in court. The privacy implications of CCTV surveillance are considered as a peripheral issue.		
Original language:	English		
English summary	http://www.parliament.uk/post/pn175.pdf		
Further information	http://www.parliament.uk/post		

Citizens' card [DBT 1994]	**Citizens' Card in Denmark**	The Danish Board of Technology	1994
Content	In 1994 the DBT conducted a consensus conference aimed at exploring the opinions of lay people towards the introduction of a "citizens card" - a smart card with a build in microcomputer with a variety of applications and with potentials for eGovernment. At the time, a plastic card had just been introduced which contained some information about the cardholder, such as name, address, civil registration number and doctor's name. The introduction of this card, which itself had only limited potential, fuelled a debate about the potential of a "smart card" with a wider range of applications.		
Original language:	Danish		
English summary	-		
Further information	http://www.tekno.dk/subpage.php3?article=265&toppic=kategori7&language=dk		

Citizens' card [ITA 2002]	**Data Prevention in Practice - Citizen's Card**	Austrian Institute for Technology Assessment	2002
Content	The purpose of this sub-project was to analyse the impacts of an ongoing project in the field of e-government. The concept in discussion was a citizens' card. It is an open concept, which describes the basic requirements for secure communication between public authorities and citizens.		
Original language:	German		
English summary	http://www.oeaw.ac.at/ita/ebene4/e2-2a29.htm		
Further information	http://www.oeaw.ac.at/ita/ebene4/d2-2a29.htm		

Colourful Flanders [viWTA 2004]	**Colourful Flanders turns to grey**	Flemish Institute for Science and Technology Assessment	2004
Content	This study dealt with the interaction between two important trends in future Western societies, i.e. the greying of society and the technology-induced transformation of everyday life. It aimed at formulating a framework of policy recommendations with regard to the elderly and ICT in 2030. To meet this objective a three-phased methodology was developed, relying on methods of participatory technology assessment and technology foresighting.		
Original language:	Dutch		
English summary	Article to be published in Poësis & Praxis, spring 2006		
Further information	www.viWTA.be		

Customer Data [TA-SWISS 2000]	**Electronic Recording and Evaluation of Customer Data**	TA-SWISS Centre for Technology Assessment	2000
Content	Not only authorities and research institutions gather and systematically evaluate Data on us - In the course of many business transactions data is electronically registered. The study analyzes what is done and could be done with these data and what are the consequences or possible consequences of their use.		
Original language:	German		
English summary	http://www.ta-swiss.ch/www-remain/reports_archive/publications/2000/38A_kf_glaeserne_kunden.pdf		
Further information	http://www.ta-swiss.ch/www-remain/projects_archive/information_society/glaeserner_kunde_e.htm		

Data Mining [ITA 2002]	**Data Prevention in Practice - Data Analysis and Data Mining**	Austrian Institute for Technology Assessment	2002
Content	The aim of this sub-project was to discuss the impact of advanced data analysis methods on privacy and data protection. The strongly increased capabilities to extract information from large data pools by data mining technologies are well known but so far rarely reflected in data protection policy. The basic questions were the relation to current data protection principles and regulations, the impact on individual responsibility for and competence to the protection of the own privacy and the identification of potential threats from widespread application of data mining techniques.		
Original language:	German		
English summary	http://www.oeaw.ac.at/ita/ebene4/e2-2a29.htm		
Further information	http://www.oeaw.ac.at/ita/ebene4/d2-2a29.htm		

Data Prevention [ITA 2002]	**Data Prevention in Practice - Individual and Societal responsibility**	Austrian Institute for Technology Assessment	2002
Content	The purpose of this project was to analyse to what extend individual responsibility, legal norms, societal agreements and/or procedures of self-regulation are necessary and practicable with regard to ensuring privacy in the “Information Society”. The study discussed the limits of individual responsibility; it identified those areas in which consumer organisations, policy makers and industry are required to reach voluntary or compulsory agreements for the protection of privacy.		
Original language:	German		
English summary	http://www.oeaw.ac.at/ita/ebene4/e2-2a29.htm		
Further information	http://www.oeaw.ac.at/ita/ebene4/d2-2a29.htm		

DRM [NBT 2005]	**Digital Rights Management (DRM)**	The Norwegian Board of Technology	2005
Content	The Norwegian Parliament has recently passed important amendments to the Norwegian Copyright Act. The process to this point has been long, and there have been many sidetracks, particularly related to the technologies affected by the act – such as Music CDs, copy protection and MP3 players. To help clear up some of the technical issues, The Norwegian Board of Technology published a newsletter on technological measures and DRM.		
Original language:	Norwegian		
English summary	http://www.indicare.org/tiki-read_article.php?articleId=121		
Further information	http://www.teknologiradet.no/files/tek_nyhetsbrev_nr_9_copy4.pdf		

Echelon [NBT 2005]	**International Surveillance and Echelon**	The Norwegian Board of Technology	2005
Content	International intelligence didn't stop when the cold war ended. The global threat of terrorism shows that there is still need for such services. One of the methods used is signal surveillance – bugging of different forms of telecommunications. The network Echelon has a special position, because it monitors non-military communication, and thus is a threat to the privacy of both individuals and companies.		
Original language:	Norwegian		
English summary			
Further information	http://www.teknologiradet.no/files/elektroniske_spor_og_personvern_190405_endelig.pdf, http://www.teknologiradet.no/FullStory.aspx?m=213&amid=177		

E-governance [viWTA 2005]	**Privacy and E-governance**	Flemish Institute for Science and Technology Assessment	2005
Content	This study deals with the rapidly growing and emerging field of E-governance applications, i.e. e-government as well as e-democracy applications. In both domains, privacy is a major issue. The general question asked was if privacy in the field of e-governance was a particular issue in the overall domain of privacy. The question was dealt within a boundary analysis, consisting of a literature research and on the basis of that research, a questionnaire was submitted to 32 (generally Flemish) experts.		
Original language	Dutch		
English summary			
Further information	www.viWTA.be		

e-Government [DBT 2005]	**Security, privacy and active citizenship in eGovernment**	The Danish Board of Technology	2005
Content	A panel of experts investigated how we are to avoid a situation where demands for efficiency and effectiveness in the public sector put citizens' security and protection of privacy at risk. In the process the group arranged two workshops, one for citizens and one for stakeholders. Through consulting with a group of citizens, it became clear that the creation of an infrastructure to exchange citizens' data must be matched with improved transparency in public administration, as seen through the eyes of the public. The expert group concluded their work in 3 general and 29 specific recommendations.		
Original language:	Danish		
English summary	http://www.tekno.dk/subpage.php3?article=1087&toppic=kategori11&language=uk&category=11		
Further information	http://www.tekno.dk/subpage.php3?article=1061&toppic=kategori7&language=dk		

Electronic Health Record [DBT 2002]	**Electronic Health Records**	The Danish Board of Technology	2002
Content	The aim of this project, conducted between January and December 2002, was to enable the citizen's assessment of the EHR, to give voice to their wishes and their worries concerning the EHR, which is being implemented in the Danish health care system. This was a participatory technology assessment project involving consultation with a citizens' lay panel and an expert panel.		
Original language:	Danish		
English summary	-		
Further information	http://www.tekno.dk/subpage.php3?article=666&toppic=kategori7&language=dk		

Electronic Privacy [POST 2002]	**Electronic Privacy**	Parliamentary Office of Science and Technology	2002
Content	This note examines the potential for commercial organisations and the public sector to infringe the privacy of digital communications, how the law can protect such communications and the implications for Government policy.		
Original language:	English		
English summary	www.parliament.uk/post/pn183.pdf		
Further information	http://www.parliament.uk/post		

Electronic surveillance [DBT 2000]	**Consensus Conference on Electronic Surveillance**	The Danish Board of Technology	2000
Content	Citizens' assessment of electronic surveillance. The increase in electronic surveillance and the related data collection and processing raises questions of what societal development the citizens want to promote. When does electronic surveillance create a feeling of security, and when does it go beyond the individuals right to privacy? The conference is conducted as a dialogue between experts and lay people and stretches over three days where it is open to the public. The final document is passed on to the members of Parliament.		
Original language:	Danish		
English summary	-		
Further information	http://www.tekno.dk/subpage.php3?article=354&toppic=kategori7&language=dk		

Electronic Traces [NBT 2004]	**Electronic Traces and Privacy**	The Norwegian Board of Technology	2004
Content	The objective of the project was to review the privacy-situation in Norway related to modern ICTs. The project focussed in particular on electronic traces made during the use of the internet and mobile phones. The project involved working with a group of experts on areas related to privacy (technical issues, law, social issues etc.), and included a focus group study involving lay people. The project resulted in a repost published in April (2004). A 4 page note to the Norwegian Parliament (Rådet til Tinget) was published in May 2004.		
Original language:	Norwegian		
English summary	http://www.teknologiradet.no/Electronic%20traces%20and%20privacy_summary_-EDms.pdf.file		
Further information	http://www.teknologiradet.no/FullStory.aspx?m=213&amid=177		

ICTs and the Elderly [NBT 2000]	**Consensus Conference on ICTs and the Elderly**	The Norwegian Board of Technology	2000
Content	The objective of this Consensus Conference was to identify the specific challenges connected with elderly people and information and communication technology and to explore how possible positive effects can be exploited and negative effects avoided.		
Original language	Norwegian		
English summary	Full report in English: http://www.teknologiradet.no/ICT%20for%20elderly%20people_wNGky.pdf.file		
Further information	http://www.teknologiradet.no/sluttrapport_eldre_og_ikt_copy_MTPIE.pdf.file		

The Municipality on the Internet [DBT 2000]	**The Municipality on the Internet**	The Danish Board of Technology	2000
Content	The aim of the project was to shed light on citizens' wishes concerning electronic information services, the possibilities of bringing about "better service in the domain of information for the citizens" in tomorrow's digital administration and at assessing these possibilities in the light of requirements concerning security and openness. Conducted using a combination of methods including focus groups and expert forums.		
Original language:	Danish		
English summary	http://www.tekno.dk/subpage.php3?article=475&toppic=kategori11&language=uk		
Further information	http://www.tekno.dk/subpage.php3?article=350&toppic=kategori7&language=dk		

Patients' Records [TA-SWISS 2000]	**Computer Based Patients' Records**	TA-SWISS Centre for Technology Assessment	2000
Content	Computer-based patient records are electronically managed health records. They are expected to be easier to manage than the often bulky files on paper, more easily available and easier to access for analyses, be it for scientific purposes, preventive medicine programs or for the insurance companies. Furthermore, computer-based patient records mean that further uses of telemedicine can be envisaged. Notwithstanding these advantages, however, potential risks, principally from the point of view of data protection and IT securiy, must also be considered when the system is introduced. The report provides detailed information about advantages and risks of computer-based patient records.		
Original language:	German		
English summary	http://www.ta-swiss.ch/www-support/reportlists/reports_temp/ta_36a_kurz_e.pdf		
Further information	http://www.ta-swiss.ch/www-remain/projects_archive/information_society/digital_patient_e.htm		

Privacy in Austria [ITA 2000]	**Endangered Privacy in Austria**	Austrian Institute for Technology Assessment	2000
Content	The purpose of this project was to analyse the data collections and processing which exist of an “average Austrian”; the results served as basic input for the “Privacy Research Programme” of ITA and as information for the consumer protection department of the Austrian Chamber of labour. The basic questions were which data are being collected by whom and what threats may result from these data pools in a dynamic perspective.		
Original language:	German		
English summary	http://www.oeaw.ac.at/ita/ebene4/e2-2a24.htm		
Further information	http://www.oeaw.ac.at/ita/ebene4/d2-2a24.htm		

Pervasive Computing [TA-SWISS 2003]	**The precautionary principle in the information society – effects of pervasive computing on health and environment**	TA-SWISS Centre for Technology Assessment	2003
Content	Information and communication technologies are constantly opening up new horizons. Current research endeavours are aimed at putting men and machines comprehensively and continuously on line, a situation often described as pervasive - or ubiquitous - computing. However, the undeniable benefits of these new technological developments and their economic potential run the risk of being offset by unwanted side effects. This study presents the outlook for the evolution of pervasive computing. It assess the risks and the benefits which developments in pervasive computing augur in terms of health and the environment, debating this issue in the light of the principle of precaution.		
Original language:	German (translation in English available)		
English summary	http://www.ta-swiss.ch/www-remain/reports_archive/publications/2003/TA_46A_2003_english.pdf		
Further information	http://www.ta-swiss.ch/www-remain/projects_archive/information_society/pervasive_e.htm		

Private Internet Use [ITA 2002]	**Data Prevention in Practice - Private Internet use**	Austrian Institute for Technology Assessment	2002
Content	The purpose of this project was to analyse the suitability for daily use of recommendations given to individual users for the protection of their privacy when using the Internet. These recommendations range from austerity in the provision of personal data to the application and use of PETs (Privacy Enhancing Technologies). The aim was to critically reflect the advice usually provided in own and other studies, searching for a possible reason for the observed divergence between expressed concerns about privacy and actual behaviour and identifying areas where individual responsibility cannot sufficiently preserve privacy.		
Original language:	German		
English summary	http://www.oeaw.ac.at/ita/ebene4/e2-2a29.htm		
Further information	http://www.oeaw.ac.at/ita/ebene4/d2-2a29.htm		

RFID [POST 2004]	**Radio Frequency Identification (RFID)**	Parliamentary Office of Science and Technology	2004
Content	This briefing provides an overview of RFID technology, its current and prospective uses, and outlines the factors limiting its uptake. It discusses measures being taken to address growing concerns over privacy.		
Original language:	English		
English summary	http://www.parliament.uk/documents/upload/POSTpn225.pdf		
Further information	http://www.parliament.uk/post		

Telecom and Internet [ITA 2000]	**Endangered Privacy in Austria - Excursus Telecom and Internet**	Austrian Institute for Technology Assessment	2000
Content	During the empirical analysis of data collections and processing which exist about an “average Austrian” (see Privacy in Austria [ITA 2000]) the use of fixed and mobile telecommunication services and of the Internet were identified as critical areas generating large volumes of data. The basic assignment of this excursus was to describe the threats for personal privacy resulting from these technologies and to develop strategies how individuals can avoid these risks.		
Original language:	German		
English summary	http://www.oeaw.ac.at/ita/ebene4/e2-2a24.htm		
Further information	http://www.oeaw.ac.at/ita/ebene4/d2-2a24.htm		

Telemedecine [TA-SWISS 2004]	**Telemedecine**	TA-SWISS Centre for Technology Assessment	2004
Content	The primary objective of this TA Study was to conduct a survey on how widely telemedical technologies and systems are currently being introduced into the Swiss health care system, together with an assessment on their future development potential (new applications). Secondly, the influence of telemedical technologies and systems have been analyzed. The study also explored the acceptance of certain telemedical applications and evaluated their medical, social, ethical, economic and legal impacts.		
Original language:	German		
English summary	http://www.ta-swiss.ch/www-remain/reports_archive/publications/2004/040924_TA_49A_e_definitiv.pdf		
Further information	http://www.ta-swiss.ch/www-remain/reports_archive/publications/2004/040923_BerichtTelemedizin_komplett.pdf		

Ubiquitous Computing [ITA 2003]	**Privacy in Ubiquitous Computing Environments**	Austrian Institute for Technology Assessment	2003
Content	One purpose of this research was to analyse the contradictions between visions of ubiquitous or pervasive computing on the one hand and the principles of current data protection regulations on the other hand. The aim was to discuss beyond direct privacy violations that result of this technology area also the long-term impacts on the building blocks of future privacy regulations. A second aim was to critically investigate the possibilities of privacy friendly design of ubiquitous computing systems; Spin-off research from technology capacity study on ubiquitous computing; based on literature review and participation in expert workshops.		
Original language:	German		
English summary	http://www.oeaw.ac.at/ita/ebene4/e2-2a24.htm		
Further information	http://www.oeaw.ac.at/ita/ebene4/d2-2a24.htm		