ENISA AdHoc Working Group

on Privacy & Technology

October 08

TECHN0LOGY-INDUCED CHALLENGES IN PR1VACY & DATA PR0TECTION IN EUR0PE

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For enquiries on this deliverable, you may contact:

Ms Barbara DASKALA at Barbara.DASKALA@enisa.europa.eu

web: http://www.enisa.europa.eu/

Technology-induced challenges in Privacy & Data Protection in Europe

A report by the

ENISA Ad Hoc Working Group on Privacy & Technology

October 2008

Authors (in alphabetical order):

Mema ROUSSOPOULOS, Foundation for Research and Technology (FORTH), GR [*WG Chair*]
Laurent BESLAY, European Data Protection Supervisor (EDPS), BE
Caspar BOWDEN, Microsoft, UK
Giusella FINOCCHIARO, University of Bologna, IT
Marit HANSEN, ULD Kiel, DE
Marc LANGHEINRICH, ETH Zurich, CH
Gwendal LE GRAND, Commission Nationale de l'Informatique et des Libertés (CNIL), FR
Katerina TSAKONA, Foundation for Research and Technology (FORTH), GR

Editors:

Marc LANGHEINRICH, ETH Zurich, CH
Mema ROUSSOPOULOS, Foundation for Research and Technology (FORTH), GR

ENISA Secretariat:

Alain ESTERLE
Giles HOGBEN
Barbara DASKALA

Contents

1. Introduction

Today, privacy and the protection of personal data are critical challenges for the development of information and communication technologies (ICT) systems and applications. This was clearly recognised in Regulation 2004/460 creating ENISA in March 2004 (Recital 8). The growth of mobile communication and wireless systems, applications relying on end-to-end Internet protocols for their dependability, and the emergence of RFID (Radio Frequency Identifiers), among others issues, create new risks of unlawful processing of personal data. Potential threats arising from both technical and human vulnerabilities (e.g., aggressive spam, malware, phishing) are becoming exploited in organised criminal attacks. The expected proliferation of sensor networks collecting information about the daily life of individuals will strain the ability to give meaningful effect to data protection principles, unless adequate means are found to guarantee compliance.

The ENISA Working Group on Privacy & Technology has been established to analyse the problems posed by these technology trends and the implications for the current EU legal framework. The main task of the Working Group is to propose actions to cope with these difficulties. In this report, we identify the main **technology-induced gaps** between data protection regulation and the realities of the developing socio-economic environment. We consider the potential threats and opportunities presented by state-of-the-art technologies and suggest priorities for tackling the most pressing gaps.

The principles of data protection are robustly formulated in technology-neutral terms, but understanding how these principles can be applied effectively to innovations supporting the Lisbon goal of making the EU "the most competitive and dynamic knowledge-driven economy" is a critical task. **If citizens are to retain confidence that their fundamental rights are protected, and that the EU framework is relevant to their daily experience, they must be able to exercise privacy rights in practical and useful ways**. We are concerned that these principles should not become merely a legal abstraction, providing only theoretical remedies for exceptional cases. If such a precarious situation is to be avoided, original thinking and decisive action is necessary.

In the remainder of the report, we provide a preliminary description of each problem identified, give a list of its specific characteristics, and offer a set of recommendations that we view as essential in closing these gaps. Our analysis takes into account the role of relevant public and private sector bodies on a European and Member State level, where applicable.

2. Recommendations Summary

This section contains a summary of the identified gaps and recommended solutions. For a more detailed discussion, see the individual gap descriptions in the body of this document.

1 PRIVACY E-INCLUSION

A critical gap is the lack of awareness and understanding of privacy issues amongst individuals as well as the lack of ability to act properly. This may divide society into "privacy-haves" and "privacy-have-nots". Just as the Information Society has to face the problem of e-inclusion with respect to information and communication technologies (ICT), i.e., how to make ICT more accessible to users, a particular focus must be on enabling citizens to protect and enforce their privacy in ICT. Of high importance are not only ICT-challenged groups such as elderly or handicapped people, but also young people with a low threshold for using ICT.

We recommend that the Commission initiates e-inclusion programmes that reach people via examples relevant to their situation in life, be it in school, in kindergarten, in a company or elsewhere. This not only requires the development of novel user assistance tools and identity management systems, but also improved communication means (e.g., privacy leaflets, education programmes in schools).

2 USER ASSISTANCE TOOLS

The best technologies and law do not help citizens if they are unable to use them in their best interest. For example, security technologies such as tools for encryption or anonymisation have not seen much adaption by end-users, despite their technical sophistication. Data controllers whose business model is dependent on monetising flows of personal data currently have not enough incentives to provide usable control interfaces for data subjects.

We recommend that research agencies and industry devote resources to the development of more useful and usable user interfaces and wizard-like guides for the proper configuration of systems and control of personal data. In order to help data subjects to better conceptualise the implications of data processing, Member States, DPAs, and consumer associations should increase their educational efforts, potentially tailored to specific citizen groups (e.g., young people, parents).

3 ONLINE SUBJECT ACCESS

One of the most distinctive aspects of the EU Data Protection framework is a strong legal right for individuals to discover what organisations know about them – the right

of "data subject access". However, and despite the fact that the reasons for which the right was originally established have grown in importance and urgency, the implementation of this right has not kept pace with other aspects of the developing Information Society, hindering it being exercised in an appropriate and effective way. The primary consideration for improving implementation is guaranteeing satisfactory authentication of the data subject making the request.

We recommend that ENISA and the Article 29 Working Party develop a detailed policy analysis for how the right of subject access could be re-framed, with a view to ensuring individuals can access a maximal amount of their personal data online, ideally for zero cost, and as far as possible consistent with the existing legal framework. User Assistance Tools and Identity Management Systems can play an important part in such a framework.

4 IDENTITY MANAGEMENT

To achieve accountability in the online world, current ICT systems generally require that users give their real name and additional personal information, proven by digital certificates. However, often the user's name is not necessary. So-called "private credentials" or "minimum disclosure certificates" provide privacy-enhancing ways to prove authorisations whilst controlling the conditions determining the user's identifiability and accountability at the same time. The availability of these technologies has implications for the interpretation of the data minimisation principle and the meaning of proportionality, i.e., that processing of personal data should not be excessive, but limited to that which is necessary.

We recommend that law and policy makers on the national and the European level re-evaluate the grounds of legitimacy for processing personal data in the light of these techniques. Further we recommend that public and private sector stakeholders contribute to setting up the necessary infrastructure for issuance and interoperability of such credentials and make use of them in their ICT systems where appropriate.

5 SECURITY INCIDENTS DISCLOSURE

Effective privacy protection is only possible if information about related security and privacy risks of the data processing, as well as the security and privacy incidents in which personal data are involved, are appropriately and timely communicated.

We recommend that the European Commission introduce a comprehensive security breach notification law. In particular it should enable not only DPAs to better identify and react to such incidents, but also individuals, so that citizens can better understand how security and privacy incidents may concern them and

to react appropriately. Further we recommend that standardisation bodies consider working on formats and protocols which support ICT systems at the user's side to interpret these notifications.

6 CERTIFICATION

Work on providing purely economic incentives to compliance has so far met with little success. Therefore work should be done on other ways of motivating compliance. For example, Member States should design tools for companies to provide certification or self-certification of compliance to data protection legislation when applying for public procurement. Member States should promote and regulate certification schemes, also involving consumers associations: tax incentives for companies compliant should be provided by Member States, and Member States should consider absolving companies from certain reporting requirements on the condition that they have privacy certification (as in the Swiss Ordinance on Data Protection Certification, DPCO/VDSZ[1], effective as of January 1, 2008). Effective sanctions (and compensation) for the violation of data protection law should be provided. (e.g., sanctions on a daily basis or punitive damages).

We recommend that the European Commission should encourage the development of privacy certification processes and develop tax and other legislation to motivate such certification. We also recommend that standardisation bodies contribute to standardise certification referentials for privacy. Supervision Tools and Best Available Techniques will be important pieces of a comprehensive certification framework.

7 SUPERVISION TOOLS

Data Protection Authorities (DPAs) face difficulties to inspect and audit the systems that process personal data. The industry does not either have adequate tools to conduct internal privacy audits. The current state of the art of technologies and legal framework do not provide the means to supervise and inspect easily the processing conducted by data controllers. Standardised supervision tools with automated and possibly remote access to DPAs should be possible to enforce inspections powers appropriately and continuously. In addition, these tools should provide non-repudiatable traceability of systems. Such tools could therefore contribute to improve the inspection processes and to ease the analysis of a privacy breach; finally, supervision tools will enhance the transparency and information about the processing that is provided to the user.

We recommend that the European Commission fund research on efficient privacy supervision tools allowing for reliable and trusted auditing; such tools should then be systematically implemented by data controllers to ensure a continuous privacy monitoring; DPAs should also use those tools in order to automate their inspections.

---

[1] *See* http://www.admin.ch/ch/e/rs/235_13/

8 BEST AVAILABLE TECHNIQUES

In order to enable the timely and effective auditing and certification of data collection and processing systems, both Industry and DPAs need an established set of sectoral Best Available Techniques (BATs) regarding privacy and security issues. This allows for a checklist-like approach for assessing privacy compliance, establishing a base-level certification upon which further analysis and supervision tools can based on.

We recommend that the Commission propose a legal instrument which will define the required structure and procedures for identifying these BATs. This instrument should foresee the involvement of all relevant stakeholders, the deliverables of which should be considered as primary guidelines by supervisory authorities and public and private organisations which implement those processing systems.

9 INCENTIVES AND SANCTIONS

There is a general gap of data controllers not being properly motivated to be compliant with data protection law. Many Data Protection Authorities are only able to check a small fraction of data controllers, so that non-compliant data processing frequently goes unnoticed. Also, given the weakness of many sanctions, the economic incentives to be privacy law compliant are often minimal.

We recommend that the European Commission and the Member States encourage an incentive system connected to a certification scheme and an effective economic sanctions system based on BATs, as well as proper auditing and supervision tools.

10 TO BE OR NOT TO BE PERSONAL DATA

Despite recent efforts by the Article 29 Working Party to clarify the notion of personal data, this concept is still often challenged. Even when the industry believes that no personal data are involved, an analysis of privacy risks should be conducted and the system should be designed in order to minimise privacy risks. In some cases, data may become personal especially if the means likely reasonably to be used to identify the person evolve as new technologies appear. Therefore, even when data is not intended to become personal appropriate safeguards should be implemented to prevent that data from becoming personal.

We recommend ENISA to develop Privacy Impact Assessment methodologies and the industry to include these Privacy Impact Assessments when defining their privacy and security policy. We also recommend the industry to develop adequate safeguards to protect one's data adequately, whether this data is personal or not.

11 SOCIAL SORTING

Social sorting such as behavioural marketing may infringe on people's privacy even if the processed data are not personal. Current regulation is scattered in different laws and does not provide an effective privacy protection in these cases.

We recommend that the Commission develops and establishes a comprehensive legal framework for all data processing affecting individuals, be it personal or non-personal. In practical terms, this could mean to demand a full audit trail of data processing and sources of data, and an obligation for better transparency for individuals concerned. Further we recommend that data controllers set up organisational and technical measures which make sure that individuals concerned can exercise their rights.

12 PRIVACY, DATA PROTECTION AND SPACE

Information Society presents a clear challenge for keeping personal data of citizens within the European jurisdiction. By digitising the personal domain but also its boundaries, the Digital Territory concept offers the opportunity to introduce the notion of territory, property and space in a digital environment. The objective is to provide tools that enable users to manage proximity and distance with others in this future Ambient Intelligence space, both in a legal and a social sense, as it is currently the case in the physical world.

We recommend that the Article 29 Working Party and the European Commission explore the possibility to apply the notion of territory to the Information Society and extend for example the principle of legal sanctuary applied to the residence to the online world.

13 FUTURE WORK

Some of the identified gaps relate to privacy risks arising from new business models which target individual consumers through *behavioural profiling*. The Working Group notes that these issues were recently raised but not resolved in the context of competition inquiries in the United States of America and in the EU, and recommends that ENISA commission further in-depth study of these issues with special emphasis on behavioural economics. The group also notes that although some supervisory bodies and the business sector claim that adequate incentives exist for satisfactory self-regulation, existing academic research[2,3] provides very little support for this view. It may be necessary to consider whether new privacy principles and market structures are required to guarantee that competitive forces reinforce (rather than undermine) privacy protection. ENISA is in a good position to promote such research, in the role of an independent facilitator of EU-wide network and information analyses, and to ensure that its conclusions are reflected in EU policies.

We recommend that ENISA commission research to continue work on privacy and technology to gain a deeper understanding. In particular, a thorough analysis should be performed concerning the market structure of online services

---

[2] *See* http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm

[3] *Tseng, Jimmy C: "An Economic Approach towards Privacy Enforcement", presentation at the PRIME/ERIM Privacy for Business Workshop, Rotterdam, December 2004. See* https://www.prime-project.eu/events/external/ERIM%20Privacy%20for%20Business%20Workshop/Tseng3.ppt

supported by advertising in general, and the economic influence of behavioural profiling in particular, with a focus on the effective application of data protection principles and the autonomy of the data subject. The study should sceptically evaluate the potential efficacy of self-regulation, and also study whether divergences in the definition of personal data are resulting in regulatory arbitrage[4,5] between Member States.

[4] *Reidenberg, Joel R., Paul M. Schwartz: Data-Protection Law and On-Line Services: Regulatory Responses, Brussels, 1998, http://ec.europa.eu/ justice_home/fsj/privacy/docs/studies/regul_en.pdf*

[5] *Bohm, Nicholas, Richard Clayton: Open Letter to the Information Commissioner, Foundation for Information Policy Research, March 2008, http://www.fipr.org/080317icoletter.html*

3. A Cautionary Tale

In this section we describe a realistic user-scenario that demonstrates many of the gaps and challenges listed in the previous section and which are further elaborated in the next section.

Sylvia has been having some privacy problems recently. For a while her favourite online portal and search engine has been displaying advertisements which seem eerily connected to aspects of her private life, moreover some of these advertisements relate to a medical condition which she has been researching online. Sylvia is concerned because she thought she had been careful not to log-in to any website she used whilst doing her research, and did not enter any other personal information which would identify her. Moreover, she is puzzled by the fact that when she clicks on some advertisements of interest to her, she receives an offer which is on less favourable terms than the offer that is displayed when she uses a friend's computer. She thinks it may have something to do with "cookies" but when she tries to understand what different types of cookie do and how to control them, she finds it very confusing. However, if she simply deletes and switches off all cookies in her browser, it becomes very inconvenient to use most of the websites she likes.

She knows that Data Protection laws in her country give her the right to discover what any organisation knows about her, but she is baffled because when she looks at the privacy policies of the websites she uses, it seems that unless she registers and logs in, the websites claim they are not collecting any personal information at all. She therefore doesn't know how to begin exercising her legal right to find out what is happening.

Sylvia sometimes gives her e-mail address and mobile phone number to websites providing online services and also to some high-street shops where she buys various products. She notices that when she visits other shops, she sometimes gets a lot of e-mail advertisements and SMS messages for products of the type she has been looking for. She begins to wonder whether these advertisements could be connected with the small electronic tags she has noticed on some of the products she buys. These advertisements also appear on her mobile phone web browser as she moves around the city, and it annoys her that she has to use the bandwidth she is paying for to browse to an opt-out page. However many times she seems to opt-out, she still seems to carry on getting quite intrusive advertisements from ever more companies.

Sylvia is an active campaigner for a controversial political cause, and although her activities are legitimate, her friend Michael (who sometimes uses her computer) has been

stopped by the police on the way to demonstrations and was asked a lot of questions when he visited a foreign country. She realises that the combination of her web browsing habits, her movements around the city, and the products she buys somehow seem to be becoming connected in ways she doesn't understand. She wonders how long this information is being kept, and if the laws of her country allow the police access, and under what conditions. Sometimes she reads stories about new such laws in the media, but they always contradict each other in the details, and seem almost deliberately confusing. On the way to the next demonstration, her car is stopped by the police, and she is questioned about some spray paint and tools she bought (using cash) at a hardware shop recently to make some household repairs, and also about why she reads a certain political website. Back at home, she notices that the items she bought carried RFID tags, but she has no idea how the police knew about the website.

She makes a call to the inquiry line for the Data Protection Authority (DPA) in her country. It turns out that the website she is interested in is based in another EU country, and she is advised to contact the DPA in that country. After quite a few e-mails to the foreign DPA, she gets a reply from someone who was able to understand her language and what she wants to do. She is advised to contact the website but she finds her e-mails to them are ignored or get an automated unhelpful response. She finally writes a letter to the website at their registered address, which isn't listed on their website, but which she eventually finds in the public register of "data controllers". However she has a problem – because she didn't have a lot of trust in that website to begin with, she registered with the website using a name she made up. After a few more exchanges with the DPA and the website, they finally agree to her request (but she has to send them her password for her account in the letter). She didn't really see why she had to give her real name and address (since she had to give her account name and password), but gave up arguing that point with the DPA and website. After sending an international postal order for 15 Euros (the website didn't accept online payment), the packet of paper she gets back a month later contains printouts of her usage of the e-mail service of the website, but nothing about "cookies" or the web surfing she did on the site when she was logged out. This was the information she really wanted in the first place (and especially how that information might have been passed to other websites or the authorities). She again contacts the DPA, who tells her that under their interpretation of the national data protection law, the website isn't required to tell her that information. Sylvia is pretty disappointed by now with how complicated it is to assert her data protection rights, and also that they turn out to be useless for finding out about the things which really affect her privacy online. She has a long list of other companies that she could write to: the shops where she bought products with electronic tags, the other websites she uses, and of course her Internet Service Provider (ISP) and mobile phone company, but it would all cost quite a lot of money in access fees, and since most of these companies will similarly claim that "they don't know who she is", she expects the same unsatisfying result. But she has a friend who is a privacy lawyer, and takes on her case. After six months of patient investigation and a blizzard of legalistic correspondence, she finally tracks down the "RFID identifiers" and cookies which she thinks must be responsible for the police asking her the questions on the way to the demonstration. But the only companies who were in a position to let the police patch together her real identity won't give her any more information, but one helpful company points her to a clause in the data protection law saying that they do not have to if she is "a suspect person".

Sylvia decides that she has completely lost control of her privacy, and she is even worried that after all her legal efforts to assert her rights, she may be considered a "troublemaker" and put on lists which could give her even more hassle in future and perhaps cause difficulty with her job, medical insurance and credit rating. She decides to give up political activity, to remove all the tags from her possessions, to get a new computer, change her ISP, close all her online accounts, and use a prepaid mobile phone, but she isn't sure how much she can still be tracked. She tells her friends about her surreal experiences with the bureaucracy of privacy, but they don't really believe her, and think she is becoming a bit of a crank. After all, they know Europe has the strongest laws protecting privacy, and it doesn't seem to be an issue that most people or the media or politicians really worry about.

However, Sylvia finds there is a new software package which works with a number of popular websites that have a good reputation for privacy protection. The package allows her to download to her computer a complete inventory of information about the interactions she has had with a website. She is surprised by the amount of detail that is stored about her surfing habits, and also notes that some of this information has been disclosed – via cookies – to other companies for advertising purposes. She chooses an ISP which participates in the scheme, which allows her to discover what "IP address" she was using at any particular time. Using this information she can go to other websites and automatically find out what information they have about her surfing on those websites (but only in some EU countries which recognise this as being "personal data"). The software package even has an analysis function which lets her compare how long different websites are keeping this data about her online behaviour, and whether it complies with the privacy policy (however she finds the policy of most sites is too vague for the software to perform this function). Moreover the software package only works with quite a limited number of websites, and some of the sites she finds most useful aren't participating in the download service. Surprisingly, some of the most innovative websites in the United States of America are beginning to enable this "attention data" download service, although she has learned by now to be very careful to look at the small print, because she realises that anyone else getting hold of this data could make inferences about some of her most private thoughts.

Her lawyer also has good news. After more than two years, she has finally won her case at a secretive "Data Tribunal" and the police have agreed she should never have been considered a "suspect person", and she is finally able to discover that a whole series of disclosures about her electronic life were made to the police by the companies she dealt with. The bad news is that all of these disclosures were made according to proper procedures (they were considered "proportionate" at the time in the light of the information available and circumstances), so she has no case against the police or any of the companies for compensation for all the inconvenience and bureaucracy (to put it mildly) she has had to put up with. Apparently, everyone "official" considers that everything was done in the proper way.

Sylvia now wonders why anyone would risk engaging in political activism to bring about social change, when the consequences can be so disturbing. She knows that democracy is an imperfect system, and justice can sometimes be haphazard, but it seems to her modern electronic life deters civic activism and has created a sinister Surveillance State.

All in all, she has had enough of politics (and life online), but she does wonder what kind of democracy her children will inherit, if everyone made the same decision. She realises she would never have understood what had happened to her without the help of her friend the privacy lawyer (whose fees she could not have afforded). Perhaps the software package for accessing and managing her own personal data would have helped if she had found it earlier, by letting her gauge the extent to which her online behaviour exposed her to privacy risks, but she reads that the software company has stopped making it. Apparently too few people were sufficiently concerned with their privacy at any given time, to make the software profitable, and the major websites she really liked really weren't interested in participating.

Links

For much more detailed scenarios see also SWAMI "Dark Scenarios" at http://is.jrc.es/pages/TFS/documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf.

4. Privacy Gaps and Challenges

The following lists the twelve major privacy gaps that the Working Group identified between data protection regulation and the realities of the developing socio-economic environment. Each section begins with a description of the identified gap, and then lists a list of challenges regarding technical research and development (R&D), legal development, and communication.

4.1 Privacy E-Inclusion

A critical gap is the lack of awareness and understanding of privacy issues amongst individuals as well as the lack of ability to act properly.

Specific Gaps

People are unaware of privacy issues or unable to protect their privacy in the current ICT landscape

Many people are completely unaware of the important privacy issues that arise from the use of new data collection technologies, social networks, pervasive technologies, etc. Others feel uneasy about some kinds of data processing, but still cannot fully grasp the potential consequences of their actions on their own privacy. Still others may be aware of the privacy issues but do not know what to do to protect their privacy. Those that want protection often decline to participate in the digital world and therefore cannot reap the benefits of the information society. Those that want to reap the benefits often give up on their privacy protection, viewing they have no choice in the matter.

Actions for redress are time-consuming and sometimes ineffective

For users that know how to maintain their private sphere, taking the necessary steps may be too costly or too cumbersome for them. The same is true for situations when their privacy rights have been violated. Actions for redress are usually time-consuming, and in several cases the effects of the privacy infringement are not revocable anyway.

The lack of awareness, understanding and ability to properly act may divide society into "privacy-haves" and "privacy-have-nots".

Usability of privacy-protecting tools is insufficient

The Information Society has to face the problem of e-inclusion with respect to ICT, i.e., how to make ICT more accessible to users. Since privacy effects in ICT are often based on user actions, the e-inclusion challenges are even more urgent if the goal is to protect users' privacy in ICT, e.g., for the elder generation or for handicapped people. Usability is an important, yet not satisfactorily solved issue when designing tools for protecting one's privacy.

The need to include young people

One particular group showing the need for privacy e-inclusion is young people, i.e., kids and teens: Young people have a low threshold for using ICT. However, in many cases they are more easily subject to seduction by services offering games or playful applications, disclosing data about themselves and possibly also about their relatives and friends.

Proposed Solutions

Raising awareness in the general public of privacy issues will need different approaches for different audiences. For example, kids have to be approached differently than elderly people. Humourless schoolbooks in an overly didactic style are not a promising means to teach privacy awareness. Instead, people must be reached via examples relevant to their situation in life, be it in school, in kindergarten, in a company or elsewhere.

Challenges for R&D

Integration of ethical and privacy needs in ICT

When developing ICT systems of any kind which may be related to processing of personal data, ethical and privacy needs should be taken into account from the beginning. ICT systems should enable people concerned to protect their privacy and exercise their data protection rights instead of bypassing large groups of the population. For age-based inclusion, work is already done in SENIOR[6] project which aims to provide a systematic assessment using dialogue as the key instrument to evaluate the social, ethical and privacy issues involved in ICT and Ageing.

The need for user assistance tools

The development of usable assistance tools such as "privacy wizards" – possibly offered free of charge by the national States to support their citizens – could be beneficial in the goal to educate users. For example, a "privacy wizard" browser plug-in could warn a user of the implications of entering personal information onto a website (e.g., mother's maiden name, identification number, etc.). Or these tools could be used for setting appropriate privacy defaults when configuring Internet access software or identity management systems. Embedding these sorts of "helper" tools directly into standard ICT systems would provide an automated means of educating users about the effects on their individual privacy.

Legal Challenges

Both the European Data Protection Directive 1995/46/EC and the e-Privacy Directive 2002/58/EC require to give specific information to data subjects. This information should not be phrased in legalese, but should be understandable by all the people concerned. For online services, Article 29 Working Party has published opinions on how to fulfil these legal demands, e.g., in WP43 and WP100. In addition, WP147 describes requirements for informing children on data protection issues concerning them.

[6] http://seniorproject.eu/

The need for legal harmonisation and enforcement

However, unfortunately these recommendations are rarely followed by now, and sometimes even basic information is missing. So it is necessary to be even more definite in describing the mandatory requirements for informing data subjects, at best harmonised on the European level. Further, best practices of ideal ways to notifying data subjects and providing further information should be highlighted in the discussion. The process of informing and making aware data subjects also should be evaluated in privacy certification programmes.

Communication Challenges

The need for public education and training

There is a need for regular broadcast documentaries with visual depictions of what could specifically go wrong. Brochures as well as audio-visual means (e.g., such as the material of "YOU decide") could thus show the potential dangers of ongoing surveillance so that people can become aware where they are monitored. Simulations should be available which show possible consequences for people releasing their personal data in different contexts. People could thus get a feeling for long-term risks for many kinds of personal data, in particular those which are more sensitive and bound to one's personality. In schools, role-plays can raise privacy awareness amongst pupils, e.g., on the possible influence of data posted in social networks on job interviews years later.[7]

Important is also the usual education within the family. Several privacy guidelines already exist in the non-digital world suggesting to parents how to impress certain messages upon their kids, e.g., to say no if their bodily privacy is imposed upon or not to accompany strangers. Parents should also be empowered to teach kids how to protect themselves in the ICT world. It may also be the other way round, i.e., kids teaching their parents or grandparents in understanding ICT effects on privacy and in using privacy tools.

Teachers, families, media and state bodies should be involved in the – probably life-long – education and learning process of all citizens which should cover how to interpret privacy-relevant information (e.g., privacy policies or privacy seals) and how to deal with privacy risks.

Links

Article 29 Working Party: Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union, 5020/01/EN/Final, WP 43, adopted on 17 May 2001,
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43en.pdf

Article 29 Working Party: Opinion on More Harmonised Information Provisions, Version: November 25 2004, 11987/04/EN, WP 100,
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf

---

[7] *This has been done in several schools on the 2nd European Data Protection Day, 28 January, 2008. See also online: http://www.coe.int/t/e/legal_affairs/legal_co-operation/_data_protection/Data_Protection_Day_default.asp*

Article 29 Working Party: Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools), 00483/08/EN, WP 147, adopted on 18 February 2008, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf

The Data Inspectorate in cooperation with the Norwegian Directorate for Education and Training and the Norwegian Board of Technology: YOU decide … Thoughts and facts about protecting your personal data, January 2007, http://www.dubestemmer.no/pdf/english-brochure.pdf

SENIOR – Social Ethical and Privacy Needs in ICT for Older People, FP7 project 2008-2009, http://seniorproject.eu/

4.2 Improved User Assistance Tools

User Assistance Tools help individuals inspect, control, and communicate their data and preferences.

Ideally, data subjects should get "ubiquitous privacy", i.e., a zero-configuration, zero-management privacy default that would allow one to freely disclosure personal data, while offering the right set of defaults to ensure the data subjects get the protection they desire. However, maintaining one's privacy and security will most likely always require an effort on behalf of the individual. This is because privacy and security are complex constructs that depend very much on the individual situation and particular context that data is exchanged or disclosed. User Assistance Tools help individuals maintain their privacy, by offering means of inspection, control, and communication.

Specific Gaps

Current tools are fragmented and scattered

Today's digital world does not offer a comprehensive "privacy suite" for end-users that supports them in managing all aspects of their privacy, but only a variety of scattered tools that typically only help to solve very specific problems.

They require considerable consumer effort to use

Moreover, most privacy technology today places a heavy burden on the data subject, expecting him or her to manage identities, obfuscate location queries, and anonymise Internet traffic – not only in front of the computer but constantly throughout the day, in situations ranging from public appearances, business events, and private meetings.

If left unchecked, most people might simply not bother to maintain their privacy

The simple notice-choice model might lead to the situation where most people simply not bother to make an effort, thus leaving privacy to be an elitist concept enjoyed by a few privacy fundamentalists. Even those who are willing to invest resources in the protection of their privacy may either be tricked into revealing more information than they planned, or simply become overwhelmed by the complexity of the data processing world.

Proposed Solutions

Assistance could mean better integrated and more easily usable technology tools that are offered to interested parties or made available in exceptional situations, i.e., when one wants to find out the details of a particular data collection. It might also take the form of an improved educational strategy that teaches citizens how to properly control and manage their privacy.

Challenges for R&D

Promote ease-of-use in user assistance tools

Ease-of-use is of particular importance for user assistance tools, since subject-access will not be used if it is complicated and/or costly (in both time and hard currency). Such tools could use "data tracking" to allow users the inspection of their personal data flows, i.e., when is their personal data released, to whom, for what purpose? System designers should be trained and educated to develop tools according to guidelines for usable conceptualisation and implementation of secure and privacy-compliant ICT systems. To ensure a correct

translation of legal regulation and language into user interfaces, Data Protection Authorities need to be involved.

Technical standards such as RFID communication protocols might also include additional references to applicable law, data collector's identity, or planned use and retention time.

Include legal information in technical protocols

Legal Challenges

For making privacy policies more accessible and understandable, different pictograms have been proposed to express privacy policy content while sparing people from studying legal jargon which may be confusing. Standardising these icons might help simplifying notice and choice. However, existing proposals do not yet focus on European data protection law.

Standardised pictograms ease legal understanding

Communication Challenges

The development of assistance tools could and should be supported by the States. In particular in areas of e-government or e-participation where the States directly involve their citizens in processing of their data, they should offer exemplary assistance tools for security and privacy and teach their citizens to use them. Data Protection Authorities could be equipped and assigned the task to support users by educating them, providing downloadable privacy-preserving configuration files or wizards where possible, giving instructions how to protect oneself in typical settings or offering a general helpdesk. Avatars might offer an interesting option to provide easier metaphors for users to understand and manage online personas and "partial identities." This is closely linked to the gaps and challenges regarding Privacy E-Inclusion, Online Subject Access Requests, and Information on Security Incidents.

Active support for user education from States and DPAs

Links

Example privacy icon sets have been proposed, e.g., by Rundle[8] and Mehldau[9].

The PRIME project has investigated requirements for user interface design in privacy tools.[10]

[8] *See http://identityproject.lse.ac.uk/mary.pdf*

[9] *See http://asset.netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf*

[10] *See https://www.prime-project.eu/prime_products/reports/*

4.3 The Right of Subject Access: Measures for Effective Implementation

Every individual has the right to access and rectification

Article 12 of the EU Data Protection Directive 1995/46/EC guarantees every individual has the right to access, i.e., the right to obtain from the controller a confirmation on whether data relating to him are being processed and information on the purposes of the processing, the data concerned, and possible recipients or categories of recipients. In addition, Article 12 grants every individual the right to obtain from the controller the rectification, erasure, or blocking of data concerning him as far as the processing does not comply with the requirements of the Directive, in particular when the data at issue are incomplete or inaccurate.

The reasons for which the right was originally established have grown in importance and urgency. The right is not merely a "backstop" to facilitate redress in particular cases, it should also function as a "grass-roots" socio-political transparency mechanism to warn policymakers if privacy is systemically threatened in some sector. Two Eurobarometer surveys in the past five years have confirmed that the awareness and exercise of subject access rights is languishing, for understandable reasons– it is frustrating, time-consuming, and inconvenient for individuals to get all the information they are entitled to, when they need it, in a form that it useful.

Specific Gaps

Online subject access facilitates more convenient exercising one's privacy rights

Subject access has become a "Cinderella" human right. The rhetoric of promoting the Information Society resonates with calls for business efficiency, innovation and citizen convenience. But if individuals want to keep track of what data is held about them, and understand the inferences made which affect how they are treated, they must overcome a legalistic obstacle course that might have been designed by Dickens and Kafka. There is a gap of offering individuals easier ways to exercise their privacy rights, in particular via online subject access which could significantly lower the threshold for individuals. But even in the case of online services, users typically do not get online access to all their personal data including those being stored in log files or being processed by profiling, scoring or data mining systems.

The primary consideration for improving implementation is guaranteeing satisfactory authentication of the data subject making the request. If the authentication process is flawed, it opens up the biggest privacy loophole of all – "pre-texted" access requests. However the ideal tool for subject access authentication is conveniently at hand: "user-centric" identity management systems, which allow the individual to manage online relationships with a plurality of unrelated data controllers, with strong mutual authentication of each party.

Online subject access should be possible in data minimising manner

In addition, there is a lack of procedures for subject access to pseudonymous data which is especially relevant in the online world with the variety of identifiers a user can have.

Proposed Solutions

Data subjects should be better supported in exercising their privacy rights, in particular in the online world. Data controllers should offer online subject access wherever possible.

Challenges for R&D

Usable design of online access to be provided by the controller

To provide convenient ways to exercise one's privacy rights, understandable user interfaces are necessary. Data controllers should not restrict the subject's access to their customer master data. Usually online reading access is not problematic provided that the user has been authenticated and the requested personal data can be shown separately from other protected information, but online rectification or erasure may often be not that easy to implement, in particular as there may be other conflicting goals. For example, users should not be able to alter audit trails or digital evidence. In particular, research is needed that allows

- structuring data controller systems to minimise the effect of exemptions (e.g., data which relates exclusively to the data subject, and does not engage other exemptions)
- strategic options to phase-in obligations on data controllers who maintain online identity relationships with data subjects, to ensure they are able to fulfil access requests online safely and to the fullest practical extent

Tools for users which support exercising one's privacy rights

In addition, users may be equipped with tools which assist them to send requests to the data controller or – if necessary – file complaints to a supervisory authority. Such tools can benefit from the functionality of user-controlled identity management and machine-readable privacy policies. Of importance are

- removal of barriers to the exercise of subject access rights, which are not appropriate to the situation of online access,
- "meta-privacy" measures necessary to protect the individual from interference or surveillance or discrimination arising from the exercise of their access rights, and
- procedures for exercising access rights against "indirect" data controllers (i.e., controllers holding data referable to individuals only by means of a pseudonymous identifier).

Data minimising ways to access own data

The right to access personal data requires some kind of identity proof so that the data are not disclosed to an unauthorised person. If a user has disclosed data under a certain pseudonym, a proof has to be given that the requesting user really is the holder of this pseudonym. This requires appropriate – data minimising – authentication mechanisms, including

- strong mutual authentication of the data subject and data controller by means of user-centric identity management technologies, adequate for submitting and fulfilling access requests online, and
- a higher level of authentication for the data subject unambiguously to authorise activation of an online subject access mechanism with a particular data controller.

Legal Challenges

Legally demanding online access

For services processing personal data in the Internet or other online scenarios, the provision of online access and other online ways to exercise one's privacy rights should be legally demanded as far as possible.

Demanding appropriate pseudonyms for data minimising access

In addition it has to be discussed whether pseudonyms which do not provide for proving the individual holdership in a data minimising way (at least without the necessity to reveal one's civil identity) should be accepted in data processing because then individuals would not be able to exercise their privacy rights. This might also require

- options for extra legal safeguards against risks of coercive subject access, and
- a framework for supervisory bodies to assess the adequacy of security measures protecting online access mechanisms and procedures.

Communication Challenges

Informing people about their privacy rights

Individuals as well as data controllers should be made aware of the data subject's privacy rights and possibilities to exercise them.

Links

The FP6 project PRIME – Privacy and Identity Management for Europe[11] proposed ways to integrate online subject access in a user-controlled identity management system.

In some countries, citizens are granted online access to their personal data in the national register file, including the logfile containing access to their data, e.g., in Belgium ("mijndossier/mondossier") and Norway ("minside").

Eurobarometer surveys on data protection:

- Data Protection, Opinion Poll, Special Eurobarometer No. 96, Wave 60.0 – European Opinion Research Group EEIG, Survey conducted upon the request of the Directorate-General Internal Market, Unit E4 – Media and data protection, December 2003, http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_data_protection.pdf
- Data Protection in the European Union – Citizens' perceptions, Analytical Report, Flash Eurobarometer No. 225, Survey conducted by the Gallup Organization Hungary upon the request of Directorate-General Justice, Freedom and Security, February 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

[11] https://www.prime-project.eu/

4.4 Identity Management for Context Separation

Purpose binding is an important legal principle in Europe

It is well known that the accumulation of personal data may yield severe privacy problems. The purpose binding principle laid down in the European Data Protection Directive strives for limiting the collection and use to prior specified purposes: "Member States shall provide that personal data must be: … (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. … (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed …" (Article 6 No. 1 of the European Data Protection Directive).

Context-spanning accumulation of personal data jeopardises people's privacy

However, also in Europe there is a trend macerating this principle so that personal data available often may also be used for other purposes even if this had been excluded in the legislative processes, e.g., it is being discussed to use toll data for law enforcement, or retention data in telecommunication for marketing purposes. This trend is amplified by more and more unique identifiers which can act as so-called "Personenkennzeichen" (personal identification number). These identifiers usually may appear in different application contexts (e.g., different sectors in the governmental area or Internet usage across various activities) and can identify uniquely the individual behind. Appearances of personal data in different contexts enable context-spanning linkage and thereby increasingly detailed profiles. This is also acknowledged by privacy experts outside Europe, e.g., Nissenbaum who discusses privacy as "contextual integrity".

Specific Gaps

The problem: increasing digital availability of linkable personal data

The increasing digital availability of personal data combined with their increasing linkability is a major problem. Even if data are anonymous in the beginning, they may be linked to a profile which then may yield enough information to identify the data subject. The increasing linkability is mainly caused by the repeated usage of unique identifiers which often are introduced by ICT systems, e.g., IP addresses, cookies or index numbers in data bases, but also the disclosure of information such as the name in different occasions may be sufficient for search engines to accumulate related information.

Enforcing purpose binding is difficult

Purpose binding is hard to enforce unless the data are already prepared for a context-specific[12] usage. Employing the data minimisation principle supports quite efficiently the purpose binding principle. There are several possibilities for restricting the data to context-specific usage,

[12] *We leave open here how fine-grained the concept of "context-specific" usage should be. In some contexts, each transaction may represent an own context, for others a coarser perspective may be appropriate. The notion of purposes may be a landmark for the discussion of contexts, but here also statutory provisions are missing.*

e.g., via sector-specific identifiers in e-government (cf. the citizen card ("Bürgerkarte") in Austria), via the use of different pseudonyms for different Internet websites, via pseudonymisation of personal data in data bases, or via so-called "private credentials" or "minimal disclosure certificates": Such credentials provide privacy-enhancing ways to prove authorisations and guarantee accountability while ensuring the user's anonymity at the same time – only in the case of misuse the user can be identified. Thus, they implement methods for accountability in the online world without the necessity for users to give their real name and additional personal information to all their interaction partners.

Poor distribution of technological solutions

Although all these solutions are discussed as components for user-centric identity management systems and have gained maturity over the last years, the concepts – in particular the more sophisticated approaches for private credentials – are not well known, and designers of applications rarely employ them in their ICT systems. Also, a societal discussion on the desired conditions of linkability and unlinkability is underdeveloped as many stakeholders haven't perceived this as an important challenge, yet, or are not aware of possible solutions.

Proposed Solutions

Challenges for R&D

Need for improving implementations

Although the maturity of the concepts for context separation and user-centric identity management have improved over the last year, there is still the need for better integration, better interoperability and better usability.

Need for building the infrastructure for private credentials

Further we recommend that administration and industry contribute to setting up the necessary infrastructure for issuing private credentials and make use of them in their ICT systems where appropriate.

Need for measuring linkability

Moreover, research should be done on the measurement of linkability and unlinkability. This is both important for ICT system design and the control of the user himself over his private sphere. In particular for long-term maintenance of privacy it is an open question how to guarantee data protection.

Legal Challenges

Evaluation of today's law in the light of private credentials

The availability of technologies for context separation has implications on the interpretation of the data minimisation principle, i.e., that processing of personal data should not be excessive, but as minimal as possible. We recommend that law and policy makers on the national and the European level evaluate today's laws in the light of private credentials.

Communication Challenges

We propose that the wished conditions of (un-)linkability and the possible legal, organisational and technological implementations are brought into focus of policy makers, developers, privacy commissioners and users. This is especially important for quite counterintuitive concepts such as the private credentials.

Trigger a societal discussion on (un-) linkability

Links

Brands, Stefan A.: Rethinking Public Key Infrastructures and Digital Certificates, MIT Press, 2000

Camenisch, Jan, Anna Lysyanskaya: Efficient Nontransferable Anonymous Multishow Credential System with Optional Anonymity Revocation, Research Report RZ 3295, no. 93341, IBM Research, Nov. 2000

Chaum, David: Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Comm. ACM, vol. 28, no. 10, Oct. 1985, pp. 1030-1044.

Clauß, Sebastian, Marit Köhntopp: Identity management and its support of multilateral security, Computer Networks 37(2): 205-219 (2001)

Jøsang, Audun, Simon Pope: User Centric Identity Management, Proceedings of AusCERT, Gold Coast, May 2005

Nissenbaum, Helen: Privacy as Contextual Integrity, Washington Law Review, Vol. 79, No. 1, 2004

PRIME White Paper – Privacy and Identity Management for Europe V3, https://www.prime-project.eu/prime_products/whitepaper/

4.5 Information on Security Incidents

Individuals can only effectively protect their privacy if they have sufficient information on the planned data processing, related security and privacy risks as well as the security and privacy incidents in which their personal data are involved.

Specific Gaps

No obligation to inform individuals about security and privacy breaches.

In the current European legal framework on data protection, data controllers are not required to inform individuals concerned about security and privacy incidents. According to the Article 4 of the Directive 2002/58[13], the obligation for the data controller to mitigate possible risks with security measures and to inform the user on these risks, is only triggered before any security incident occurs but there is no communication obligation after the incident takes place.

The legislator might think that the competitive environment together with self-regulatory process would have completed the legal framework with the implementation of technical and organisational safeguards requested for the proper management of security incident. However, it appears in light of critical and illustrative incidents that these first incentives are not enough for promoting the need to notify the end user of security breaches and to mitigate proactively their negative effects.

The lack or even absence of incident notification also undermines the implementation of preventive measures which are requested by today's legal framework.

Another direct consequence of the absence of notification and information on security incidents is the production of figures and statistics which are not reliable and which do not contribute to a more trustworthy and transparent environment.

Even if information is available on the fact that a security breach occurred, people usually neither know how they might be affected by such an incident nor how to react in an appropriate way.

Proposed Solutions

Challenges for R&D

Security feeds as a standard reporting format

Basing on news feeds for reporting security-relevant vulnerabilities, e.g., by Computer Emergency Response Teams, a prototype of a "security feed" has demonstrated how information on security and privacy threats and incidents can be transferred in a structured XML format via an RSS feed to be interpreted by the identity management system of the project PRIME – Privacy and Identity Management for Europe. This concept comprises all mechanisms and implementations in use such as protocols, applications, cryptographic

[13] *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.*

algorithms, as well as the identity management system software itself. In particular users are informed about the risk to their private sphere, i.e., who definitely or potentially has unauthorised access to personal data, and about the consequences, e.g., options to take action.

Legal Challenges

We must legally oblige data controllers to notify security breaches.

The data controllers themselves should be legally obliged to inform people individually or via broadcast media on incidents – similar to the Security Breach Notification Acts in many U.S. States.

In November 2007, the European Commission issued a proposal[14] for reviewing the Directive 2002/58 and introduced the obligation to notify security breach.

Privacy incidents also relevant

Note that the discussion usually focuses on security incidents only, e.g., hacking attacks or lost data. There might be other privacy-relevant events such as the fusion of companies which join their databases or the change of the country where personal data are being processed. This kind of information may also be relevant to the individual's privacy.

Communication Challenges

Incident communication enables citizen privacy management

People should be informed in an understandable way about security and privacy incidents which may relate to them or their data. They also should be given advice in each individual case on the actions to take to minimise undesired effects to their privacy. This kind of information enhances the transparency of actual privacy-related data processing and acts as a basis for individuals' management of their private spheres.

A more accurate and exhaustive reporting of security breaches would permit to promote post-incident solid safeguards and well tuned compensation measures for managing the residual risk.

Multiple distribution channels for incident reporting

Not only the data controllers themselves, but also other parties such as newspapers, Data Protection Authorities, consumer protection organisations or peers could distribute available information on security and privacy threats or incidents. This kind of information could be transmitted in a standardised digital format which makes it easier to be interpreted by the user's computer. In particular a combination with user-controlled identity management systems creates synergies.

---

[14] *Proposal of 13 November 2007 for a Directive of the European Parliament and the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, and 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.*

Links

Security Breach Notification Laws: Views from Chief Security Officers A Study Conducted for the Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, December 2007, http://www.law.berkeley.edu/clinics/samuelson/cso_study.pdf

Hansen, Marit, Jan Schallaböck: Extending Policy Negotiation in User-Controlled Identity Management by Privacy & Security Information Services, Position Paper Submission to the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, http://www.w3.org/2006/07/privacy-ws/papers/18-hansen-user-controlled-idm/.

Hansen, Marit: Marrying Transparency Tools With User-Controlled Identity Management. In: Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci (Hrsg.): The Future of Identity in the Information Society, Proceedings of the Third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on The Future of Identity in the Information Society, August 2007; IFIP International Federation for Information Processing, Volume 262; Springer; 2008, pp. 199-220

Hogan & Hartson Analysys: Preparing the Next Steps in Regulation of Electronic Communications − A Contribution to the Review of the Electronic Communications Regulatory Framework. http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/next_steps/regul_of_ecomm_july2006_final.pdf.

Nageler, Antje: Integration von sicherheitsrelevanten Informationen in ein Identitätsmanagementsystem. Diploma Thesis, Christian-Albrechts-Universität zu Kiel, May 2006.

4.6 Guidance on Certification Schemes

Certification Schemes can aid compliance verification

One of the main problems facing the information society today is a lack of transparency in ICT products and services developed with respect to their compliance to security and privacy standards. For users, data controllers, and DPAs, privacy compliance is one of the main challenges of ICT systems. Certification schemes should ensure that a product or a service has been designed and can be used in compliance with European legislation on data protection.

Specific Gaps

Today, no such privacy certification exists

The availability of trustworthy ICT solutions in general and particularly of data privacy and security enhanced technological applications today is equally important for all players across the EU. Attention therefore should be focused on developing the means and criteria necessary for making available such trustworthy and privacy compliant certification schemes in a harmonised manner in all Member States.

Certification schemes make privacy protection more effective

In this section the discussion to follow shall illustrate the existence of this gap along with the respective requirements to be met and the impact/advantages to be gained. The latter include competitive advantages, trust enhanced in certified products, public trust and awareness raised, the promotion of privacy by design rather than as an afterthought, and the application of data protection principles in a homogenous manner and thus more effectively, for all information society players concerned (data subjects, data controllers, Data Protection Authorities, ICT developers, vendors, manufacturers, Member States, etc.).

A minimum level of protection of personal data should be set

We stress here that (a) such certification schemes should ultimately guarantee that a specific product meets a certain (minimum) level of protection of personal data, that (b) there is a need to develop a methodology to serve that purpose, as well as to promote adoption of such certification systems, and that (c) standardisation bodies need to standardise certification referentials, criteria and conditions used to assess privacy compliance.

Proposed Solutions

There need to be incentives for certification

Member States should promote and regulate certification schemes, also involving consumers associations: tax incentives for compliant companies should be provided by Member States, and Member States should consider absolving companies from certain reporting requirements on the condition that they have privacy certification.

Having considered whether such a certification system should be mandatory or not, who should endorse adoption of such systems, and how to be transparent in reaching a general consensus on what privacy requirements should be met in order to fill in this gap, new solutions to motivate compliance should be examined. For instance, Member States should design tools to provide a voluntary certification or self-certification of compliance to data protection legislation when applying for public procurement.

Already experiences with certification schemes exist

We suggest that ideas should be taken from lessons learned through similar research projects (e.g., EuroPriSe[15]) and other countries (e.g., Switzerland[16]) that have developed such certification schemes, as well as past experience gained in accredited electronic signatures, encryption related technologies and their respective legal frameworks.

Key characteristics of a privacy certification scheme

We suggest that such a certification scheme should have the following key-characteristics: those parties willing to be known to the public as accredited privacy and security certifiers should be previously certified for that purpose by certain independent (third) parties that have been already established as dedicated accreditation bodies (in cooperation with DPAs).This certification should occur once they have met the respective technological and legal requirements (privacy by design, Best Available Techniques, minimum of privacy principles) set out in the respective regulations issued by DPAs in cooperation with the Article 29 Working Party and the European Commission. The duration of such a certificate should be for a certain period of time, no more than two or three years, for instance, during which annual evaluation of compliance should be envisaged. In case of violation, misuse, misrepresentation or misappropriation of this certificate, penalties and fines should be imposed let alone cancellation of this certificate. There is thus a need for further legislative steps be taken to this direction at a Commission level to facilitate a harmonised implementation and application across the European Union. In particular, controls and liability of the evaluators and the certifiers should be defined.

International standardisation needed

Finally, the certification referential schemes should be standardised at the international level to ensure harmonisation and transparency of the methodologies used and of the criteria assessed. This referential should contain the criteria to be checked when evaluating the products or services concerned. They should serve as guidance to evaluators on how to assess ICT products and services.

---

[15] *See* http://www.european-privacy-seal.eu/

[16] *See Ordonnance sur les certifications en matiere de protection des donees (OCPD), 28 September 2007, Le Conseil federal Suisse, and Loi federale sur la protection des donnees (LPD) du 19 join 1992 (Etat le 1er Janvier 2008), L' Assemblee federale de la Confederation Suisse. See* http://www.admin.ch/ch/e/rs/235_13/index.html

4.7 Supervision Tools

Tools are needed to perform internal privacy auditing

Companies that process personal data must specify their privacy policy and ensure that it is properly implemented in their environment. This privacy policy may indeed be very complex due to the great number of parameters to be considered. Once this policy is deployed, scalable and automated compliance checking solutions should be performed continuously, however adequate supervision and management tools are not available to the industry that lacks efficient tools to conduct internal privacy auditing.

These are also useful for supervisory authorities

In addition, Data Protection Authorities (DPAs) have continuously faced difficulties for implementing controls and conducting audits on the personal data registered, processed and used. Finally, although the European legal framework defines detailed obligations and safeguards data controllers need to implement and follow[17], it does not provide practical supervision tools or does not ask for the development of such tools for the benefits of supervisory authorities.

Specific Gaps

Individual privacy auditing is highly resource intensive

Most of the ICT systems which process personal data are usually not designed for facilitating audit exercises or even self-auditing activities. The tools for such supervision need then to be tailored on a case by case which request additional resources. This requires an ability to verify the compliance of a physical implementation privacy policy to a high level privacy policy. Therefore, dedicated metrics need to be considered for privacy, and certain means to map high level specifications to physical configurations within the information system should be included.

In addition, given the huge volume of data collection activity to be audited, it is therefore crucial that standardised and non-repudiatable logging techniques be developed to allow for reliable automated auditing.

Supervision tools would be useful for industry, DPAs, and users alike

These tools could then possibly be considered to be made available to DPAs, to assist them in enforcing their inspection powers on a continuous basis and possibly remotely. The end user should also be in a position to obtain automatically feedback on the way his/her personal data are processed.

Proposed Solutions

Challenges for R&D

Sticky Policy paradigm

Privacy policies could be applied to the transferred data (e.g., encapsulated as "sticky policies") so that data controllers would be obliged to respect what is stated therein. For transparency reasons, this also would require

[17] *See as an illustrative example the Article 17 of the Directive 1995/46*

that not only – as legally demanded today – recipient categories be documented, but accurately the real recipients.

Synching technical and legal privacy policies through audit trails

Effective automated audit tools of data protection practices would make it easier to enforce policies. Audit trails could be included proactively in the systems to enable reverse-engineering of a technical privacy policy and check that it complies with an acceptable high level privacy policy.

R&D on more automatic tools for control, traceability and audit operations should be encouraged. Another path could be to outsource this activity to accredited (private) bodies able to conduct such activity and provide certificates to organisations meeting privacy requirements (see, e.g., the certification scheme implemented in Geneva canton, Switzerland).

Defined checkpoints simplify verification

Both internal auditors (such as the auditing department) and external auditors (such as the DPA in charge) could profit from defined (and possibly standardised) checkpoints in ICT systems and data processing workflows. Moreover, the testing procedures used in an audit should cover all relevant cases. For a long-term supervision even specific dummy data could be inserted to see whether these data leak and later appear outside of the ICT system. This means that careful attention must be given to ensure that these dummy test data do not become an uncontrolled digital identity themselves with misuse potential.

Legal Challenges

Require audit trails along the entire data trail

It would be possible to legally require that processing of personal data be only allowed if the data come from a trustworthy source where all data transfers have to be documented.

Remote access for DPAs

Remote and permanent access by DPAs to limited features of privacy supervision tools used by data controllers could be considered to verify that the systems comply with the notifications and to facilitate inspections.

Communication Challenges

Internal testing through self-auditing

Self-auditing reports would also contribute to the effective execution of the tasks of the supervisory authorities that will be able to identify the weakest spots and to focus on them during their own auditing procedure.

4.8 Guidance on Best Available Techniques

BATs are a particular combination of technologies, protocols, and standards

Privacy and security are complex issues that will hardly be solved once and for all using some kind of universal technical solution. Instead, different application areas call for different technical support to provide privacy to citizens. Such technical support must also be carefully complemented with legal frameworks and practical guidelines that specifically target a particular application domain or selected set of operational principles. We can call this particular combination of technologies, protocols, standards, practices, etc., that can provide a reasonable level of privacy protection in a particular area "Best Available Techniques."

Specific Gaps

BATs for privacy and security need to be defined and harmonised

There is a gap of defining and then harmonising – at the European level – what the Best Available Techniques (BATs) in various domains are, and to what extent they should or must be employed by data controllers and processors.

Example: Location Privacy

The current discussion around location privacy techniques may illustrate this gap. Many of today's location privacy proposals try to hide location requests in an area large enough to hold at least *k-1* other users. This is called "*k-anonymity*." However, while a powerful technique, it is important to more specifically address the practical use of such techniques. How can a user employ, say, a *k-anonymity* technique? How would one be able to judge what value of *k* is appropriate, or when to turn the system on or off? How would one strike a balance between location precision and location privacy? Or should we simply adopt a trusted third party model where all data is centrally administered by, e.g., the mobile phone provider, and we use statistical database approaches and other tools to protect user profiles? Different application scenarios might require different answers.

Proposed Solutions

Creating a set of BATs in the area of data protection is both a question of finding suitable techniques, and establishing a process to harmonise these across European Member States.

Challenges for R&D

Identify and group technologies and practices

A first step would need to identify the sets of relevant applications, in particular those grouped around novel technological developments (e.g., RFID, Location Based Services, and biometrics). These should be further grouped according to their respective information flow models, i.e., their particular data processing practices and information needs.

Find suitable sets of techniques by specific application domains

Once generic application types have been identified, one can survey current technologies and practices and provide a well-defined set of best available techniques for such applications of such a type. As defined above, economic and technical viability are important factors in such an assessment.

Legal Challenges

Address DPA involvement and enforcement models

Data Protection Authorities (DPAs) have to be involved in this process of identifying and enumerating privacy and security BATs. It has to be determined how DPAs can and should enforce the usage of BATs, in particular if technologies are available, but not part of standard systems (e.g., secure deletion through wiping tools that are not part of standard operating systems) or if their use requires either the cooperation of multiple parties or an additional infrastructure (e.g., anonymising systems to protect personal data before they are noticeable by a specific data controller cannot be operated by this data controller itself, but need additional independent providers).

Anticipate future combinations of technology

Note that solutions have to take into account the risks created by the combination of several existing technologies, i.e., these have to be anticipated, analysed and quantified. For example, major risks arise when combining facial recognition biometrics with video surveillance tools or Location Based Services with cartography information. When defining a policy with respect to a specific technology, future uses should therefore be foreseen as much as possible so that adequate purpose limitation safeguards can be included at each technology's design phase.

Communication Challenges

A public process

The list of identified BATs for important application settings and their characteristics need to be made public, so that every data controller and processor can be aware of them. Best Practices could also illustrate the usage of BATs.

Links

BATs have successfully been defined within the environmental context, given by the IPPC Directive 96/61/EC[18].

The BSI (Bundesamt für Sicherheit in der Informationstechnik; the German Federal Office for Information Security) recently launched a project which could constitute an illustrative example of BATs for RFID applications.[19]

[18] *See http://ec.europa.eu/environment/air/legis.htm#stationary*

[19] See http://www.bsi.de/presse/pressinf/071207_RFID.htm

4.9 Effective Incentives and Sanctions

Privacy laws are often not followed

Data protection law has quite old roots. However, today's data processing world often shows a lack of compliance of ICT components and organisational structures with data protection law. It could be seen in the past decades that when relying solely on free market forces, privacy-enhancing technologies do not evolve on a large scale.

Specific Gaps

There is a lack of motivation and not enough incentives

There is a general gap of data controllers not being properly motivated to be compliant with data protection law. Closely linked to this gap is also the lack of motivation to employ privacy-enhancing technologies, which would bring forward the state of the art.

A lack of tools makes it hard for DPAs to check compliance

In general, sanctions against non-compliance can only be imposed if the supervisory authority in charge or a court becomes aware of the infringement of data protection law. Today, Data Protection Authorities only check a small fraction of data controllers so that non-compliant data processing frequently goes unnoticed.

Today's economic scales provide not enough incentives to follow the law

Given the weakness of many sanctions, the economic incentives to be privacy law compliant are often minimal. For example, data controllers in some jurisdictions can only be fined once – even if they do not change their data processing, they only have to pay a fine once. In several cases, courts have also withdrawn the obligation to pay a fine to avoid having to check all competitors of the accused data controller when faced with discrimination charges.

Proposed Solutions

Compliance through rewards or punishment

To encourage data controller to improve the privacy of their data subjects, two general solutions are possible:

1. Providing *incentives* which reward the data controller
2. Providing *sanctions* which punish the data controller

Effective sanctions differ between private and public entities

What can be an incentive or a sanction may depend on the kind of data controller. For example, for companies economic drivers matter most. This also means that a fine to sanction non-compliance with data protection regulation has to be noticeable by the company – it should not pay off for the company to behave in a privacy-invasive way. For governmental processes, processing *must* be compliant with data protection law – otherwise regulatory supervision should intervene immediately.

Challenges for R&D

The lack of automated audit tools makes law enforcement against breaches minimal. Such tools would require a certain standardisation and certification process that would identify, in cooperation with Data Protection Authorities, the set of information required for such an audit trail.

Standardised auditing tools are needed for effective compliance testing

Legal Challenges

Procurement conditions in the public service could require a privacy-compliant design or a certification or self-certification. Certain technological measures could be regarded as compulsory as they already are in some jurisdictions; though it remains to be defined which measures would be beneficial.

Compulsory certification or use of privacy technology

Effective sanctions could help to convince data controllers that they should implement privacy-compliant systems. Sanctions should not be limited to administrative ones (in some countries sanctions are also provided by criminal law) but should include also an efficient liability system. In this case, consumer associations may play an important role.

Effective and noticeable economic sanctions

However, in many Member States the sanctioning system does not work effectively. The sanctioning system should be supported by an efficient audit system. On the other hand, incentive should also be provided. They may include, for instance, tax incentives. This requires and is closely connected to a certification system.

We recommend that European Commission and Member States encourage an incentive system connected to a certification scheme and an effective economic sanctions system.

Communication Challenges

Privacy compliance or the (proven) design according to privacy-enhancing criteria can be a unique selling proposition for a data controller. This also supports establishment of a good reputation which can help attract and bind customers. Privacy-awareness campaigns could create a market demand for privacy-compliant systems, in particular if there are convenient ways for customers to express their demands for privacy. Less personal data means less risk of misuse which also is good for the reputation of the data controller.

Campaigns to create consumer demand for compliance

Data controllers could be convinced that the privacy-enhancing organisation of data processing, in particular according to the data minimising principle, is often cheaper than having to provide not only storage media, but also appropriate safeguards, documentation, and subject (or law enforcement) access.

Explain the benefits of anonymous data

Links

Ross Anderson maintains an "Economics and Security Resource" page on his website.[20] Alessandro Acquisti offers a similar site on the economics of privacy.[21]

[20] See http://www.cl.cam.ac.uk/~rja14/econsec.html

[21] See http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm

4.10 To Be or Not To Be Personal Data?

The notion of personal data covers all information which can be linked to an individual

According to Directive 1995/46/EC, personal data shall mean any information relating to an identified or identifiable natural person ("data subject"). This notion is very wide so as to cover all information which may be linked to an individual. In fact, many different data can be combined and may contribute to the identification of a given person (e.g., through social networking, by monitoring RFID tags, by combining search queries on search engines, etc.). Even though European lawmakers have adopted a broad notion of personal data, this notion is not unlimited. The scope of the data protection rules should not be overstretched, but unduly restricting the concept of personal data should also be avoided. Since the border between personal and non personal data can sometimes be blurred, efforts have been made to clarify the notion of personal data, such as the Article 29 Working Party's opinion on the concept of personal data.

Specific Gaps

It is not always clear if data is personal or not

The concept of personal data is often challenged, despite the recent efforts by Article 29 Working Party to clarify this notion. This is problematic: When data is not intended to be personal, there are not necessarily sufficient safeguards to ensure it does not become personal.

Example: RFID tags in the retail are not deactivated even if the tag has no intended purpose beyond the point of sale

Further, acceptable intrusion in one's privacy and user perception of personal data are dynamic concepts. For instance, RFID technology is used in many applications nowadays (including retail, digital identity in passports, car keys, mobile payment, etc.). This technology introduces numerous threats since it could allow user monitoring and data collection possibly anywhere and without the person's knowledge. It can identify a natural person when data such as the person's name or biometric data is stored on the tag. An individual could also be tracked, traced, and profiled, through his tagged items containing unique numbers. In the retail, since the data contained in a tag is usually not intended to be personal when it is used for logistical purposes, the tag is usually not deactivated at the point of sale so the user carries items containing active tags that could be used to track him.

In addition, acceptable intrusion in one's privacy and user perception of personal data are dynamic concepts which evolve in time according to social, factors, expected security requirements and technological improvements. Social factors enter into personal reactions to privacy-invasive technologies since the definition of one's private sphere is subjective and depends on one's age, culture, and environment. Expected security requirements also differ since expert users may wish to configure their systems accurately whilst the majority is likely to prefer simple, understandable and privacy-compliant default settings. Finally, data which would be considered today as non-personal (since the means required to make them personal would be excessive) may become personal if technological evolution makes those means reasonable.

Proposed Solutions

Challenges for R&D

Develop appropriate technological safeguards, even for data that is not intended to become personal

To assess privacy risks related to data processing, Privacy Impact Assessment methodologies should be developed and applied. The complexity of the analysis to be conducted should depend on the sensitivity of the processing and of the data concerned.

Safeguards should be developed to protect one's data adequately, whether this data is personal or not. This will significantly improve user empowerment and control.

Technological means and evolutions should be anticipated appropriately when designing systems and when defining regulations, so that data that is not intended to be personal does not become personal when technology evolves.

The social impact of new technologies should be systematically and scientifically assessed; the usefulness of technology should be demonstrated.

Legal Challenges

Regulation should ensure that non-personal data may not become personal

Regulation should ensure that data is protected adequately especially if there is (or if will be) uncertainty that it could become personal.

However, as a form of exercising the right to privacy and the right to data protection, the right to anonymity has to be continuously balanced with other fundamental rights. As anonymity usually cannot be absolute, space should also be left to forms of "reasonable" anonymity.

Especially when sensitive data is concerned, adequate anonymisation schemes should be used when possible.

Once the law has established a right, balancing it with other rights, technology should implement the rules. The effectiveness of a right to anonymity must be guaranteed through technology and technology should provide for the protection of different degrees of anonymity.

The requirement to conduct a Privacy Impact Assessment could be included in the legislation.

Where a Privacy Impact Assessment shows significant privacy risks associated to the processing, the legislator could impose appropriate privacy safeguards to be implemented to mitigate those risks.

Communication Challenges

By improving understanding of user-empowerment technologies and of the need to protect one's data, awareness campaigns will improve user practices and will thus contribute to mitigate the risks faced by EU citizens in the online world.

Awareness raising will mitigate the risks faced by EU citizens in the online world

By systematically using harmonised Privacy Impact Assessment methodologies and processes, the industry will improve transparency, mitigate privacy risks related to the data they process, and thus benefit from increased trust in the technology by the users.

These campaigns will also trigger a public need for comprehensible and efficient privacy enhancing technologies.

Links

Directive 1995/46/EC[22] defines personal data and the legislative framework to be applied to it.

The concept of personal data has been clarified and discussed in detail in 2007 in an Article 29 Working Party opinion[23].

[22] http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

[23] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

4.11 Privacy Protection and Social Sorting

Social sorting may infringe on people's privacy even if the processed data are not personal

In many cases, a unique identification of individuals – i.e., personal data – is not sought by data controllers because processing concentrates on population groups, aiming at some kind of categorisation, also known as social sorting, stratification, segmentation, or classification. This may be done by profiling or scoring techniques for various purposes such as marketing, determination of creditworthiness, price discrimination, and decision making in e-recruitment, the health sector, or criminal investigations. In these cases, the data themselves are often not considered personal data because they do not relate to specific individuals, i.e., the data controllers do not know the name of the individuals whose data are being processed. However, the consequences of this data collection and analysis often impinge on individuals and thereby affect their privacy. The provisions of Article 15 of the European Data Protection Directive on automated individual decisions are not meant to cover these constellations.

Specific Gaps

No transparency of social sorting for individuals

The main gap is that individuals often are not aware when they are subject to social sorting and how specific decisions concerning themselves are reached. This means they neither know whether the data on which the social sorting is based on are correct nor whether the algorithms and implementations of scoring and other analysis tools work properly. In particular the entity which generates decisions on individuals may not be the same as that which collects and aggregates the information which makes it harder for individuals concerned to address complaints and achieve remedy. Furthermore, in predictive scenarios it is usually not possible for the individual to prove the forecast wrong.

Exercising individual privacy rights does not work with non-individual data

As far as the data processed is not considered as personal data, this also weakens the possibility of exercising one's privacy rights (access, rectification, erasure of personal data if illegally stored, revocation of consent). This would require a proof that the data in question belong uniquely to oneself as individual. For example there are cases where the data protection right to access has been denied when dealing with cookie data only because a cookie is not necessarily uniquely bound to one individual. This shows that many identifiers bear a sufficient quality of linkage to yield information desired by the processing entity, but do not enable individuals concerned to exercise their privacy rights.

Reachability may facilitate direct manipulation

In addition, there are settings where the individual may be addressed and reached, e.g., by a telephone call, an e-mail or personalised advertisement via television or website. In particular those kinds of marketing which aim at seducing potential customers can be manipulative and infringe on the individual's privacy. It also may provoke a reaction which enables the processing entity to refine the collected data or establish the personal linkage.

Proposed Solutions

The right to informational self-determination can only be fulfilled if individuals can know about all data processing concerning them.

Challenges for R&D

Full audit trail for all data processing

One solution is an organisational and technical framework which makes sure that individuals concerned can protect themselves and can exercise their rights. This may require the preparation of a full audit trail whenever data – be it personal or non-personal – are being processed as far as this may impinge on individuals. This would mean that each step of data processing with all input and output including the information on responsible parties for data, algorithms and implementations can be made transparent to individuals concerned or to parties trusted by them. By this means, incorrect data or flaws in data processing could be identified and corrected more easily.

The organisational and technical framework is even more necessary considering the upcoming ambient world with a variety of sensors, communicating which each other and collecting information on their surrounding – including individuals. Here, transparency enhancing technologies could support individuals concerned [Hildebrandt/Koops 2007].

Legal Challenges

Consistent legal framework for all data processing affecting individuals

Current regulation concerning this gap seems to be scattered, e.g., some parts are in data protection law, others in non-discrimination law and yet other parts seem to be not fully handled. Therefore, the main legal challenge is the development of a consistent and comprehensive legal framework for all kinds of personal and non-personal data processing which may affect individuals. This framework should especially contain an obligation for better transparency and understandability of data processing for the individuals concerned.

Communication Challenges

Informing individuals about data collection and analysis

Individuals should be made aware when they unwittingly leave data trails, what information about them is being gathered and linked by different parties, or when they are – possibly mistakenly – held responsible for specific actions. Further, they should be informed on how to react best if they feel treated in an unfair way concerning their privacy.

Links

Hildebrandt, Mireille, Serge Gutwirth (Eds.): D7.4: Implications of profiling practices on democracy and rule of law, FIDIS Deliverable, Frankfurt a.M., Germany, September 2005, http://www.fidis.net/fileadmin/ fidis/deliverables/fidis-wp7-del7.4.implication_profiling_practices.pdf

Hildebrandt, Mireille, Bert-Jaap Koops (Eds.): D7.9: A Vision of Ambient Law, FIDIS Deliverable, Frankfurt a.M., Germany, October 2007,

http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf

Lessig, Lawrence: Code and other laws of cyberspace, Basic Books, New York, 1999

Lyon, David: Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination, Routledge, 2002

Phillips, David J.: Privacy policy and PETs – The influence of policy regimes on the development and social implications of privacy enhancing technologies, in: New Media & Society, Vol. 6, No. 6, SAGE Publications, London, Thousand Oaks, CA and New Delhi, 2004, pp. 691-706

Article 29 Working Party: Opinion 4/2007 on the concept of personal data, June 20 2007, 01248/07/EN, WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

4.12 Privacy, Data Protection and Space

A lack of boundaries in the digital domain

Territorial privacy has long since played an important role in privacy protection ("my home is my castle"). A territory is usually a continuum in space; the real and digital elements of a person, however, may co-exist in disparate locations (in the end, any digital element is recorded on a hard-disk or other medium which has a specific physical substance and location – although the latter may change with time, i.e., if the device is mobile). This lack of clear territorial boundaries in the digital world leads to both specific legal problems and general problems of perception when managing one's privacy.

Specific Gaps

The need to keep personal data of citizens within the European jurisdiction

According to Article 25 of the Data Protection Directive 1995/46/EC, personal data usually may only be transferred to third countries if that country provides an adequate level of protection. There are exceptions such as transfer to companies in the United States which adhere to the Safe Harbor Principles.

However, in all cases outside the European jurisdiction, the defined adequate level of privacy protection does not take into account the possibility of access of national security agencies. This means that all data in those countries may be subject to access and analysis by these agencies which may have undesired consequences for individuals as well as organisations, e.g., companies whose trade secrets may be exposed.

Physical vs. digital

In the Information Society, there is a lack of territoriality and therefore no protective boundaries. At the same time, there is a multiplication of invisible and uncontrolled bridges between the real and the digital environments. If we still have the tools in the physical world to manage our privacy (through distances) it is not yet the case in the digital world but this new environment is becoming through the growing number of bridges an inherent part of our everyday life space.

Legal rules, tacit socio-cultural norms, and even traditions constitute the guidelines for people's understanding of what is private or public space or of what is socially accepted as private or public space. Although the distinction between the two spaces is not always that clear, people are aware that boundaries do exist and they act accordingly (e.g., a fenced private land, the 'keep out' sign on someone's private lawn, the questioning or annoyed look given to strangers in a neighbourhood bar).

Perceiving space in cyberspace

Although people have an intuitive sense of privacy violation in physical space, they do not have a similar sense in cyberspace. For example even in public spaces if someone eavesdrops, it is clear that there is violation. In cyberspace it is not clear whether someone is eavesdropping nor if this is a violation of privacy. How can these boundaries be made more explicit in cyberspace?

Remote storage complicates the notion of spatial boundaries in cyberspace

In this context and without underestimating the already complicated nature of privacy in the physical space and the difficulty of protecting it appropriately, it seems that in the digital space, privacy is far easier to violate and more difficult to protect than merely shrugging off an undesirable touch. Moreover, the default in cyberspace is more likely to be privacy-invasive, thus always requiring appropriate action from the user. Consider for example when upon installing a programme or signing-up for an online Internet service, you are automatically subscribed to newsletters or services, and you are subsequently informed that you should go to the respective website and request to be unsubscribed. Consider also a photo album kept in a cupboard of our living-room, which is supposed to be only viewable by the members of the household, including the friends and relatives that may see it; however, a digital family photo album, sometimes available and even searchable over the Internet, usually is not equally protected[24].

The opt-out possibility for these kinds of applications is thus most of the time made more difficult and requires extra effort on the part of the user, as well as technical knowledge. To make matters worse, the user is often not aware of the amount and the type of information (e.g., IP address, cookies, web-tracking, cache, search terms etc.) that is captured as one surfs the net or performing other online activities, thus making it more difficult to opt-out or to protect one's privacy.

Virtual worlds

So called virtual worlds constitute another manifestation of this lack of clarity. Some predict that virtual worlds will soon be used by mainstream companies. Applications such as Kaneva are appearing where social networks and virtual worlds converge. There are many unexplored privacy issues here. For example what is the legal status of virtual financial data (e.g., LindenDollar accounts)? Another interesting question is what would be the meaning of issuing an ID card for an Avatar – the point being that even purely digital personae may benefit from strong authentication combined with linkability control. The avatar as a metaphor for a partial digital identity may also be a useful privacy user-interface tool.

[24] *A good example is the case of not well configured so-called online "social networking" applications, such as mySpace.com, Flickr, YouTube, Facebook, which allow for online storing, sorting, sharing but most importantly searching of photos and videos.*

Proposed Solutions

Challenges for R&D

Data storage and infrastructure within EU jurisdiction

To protect the personal data of European citizens, mechanisms should be applied which keep their data in the European jurisdiction wherever possible. For Internet search engines this could be achieved by offering proxies for outside services or providing separate search engines.

Similarly critical infrastructures should be implemented within the European jurisdiction only and avoid dependencies from other nations.

Legal Challenges

The data handling within these European services would have to adhere to European data protection law which would prevent unnecessary storage and usage.

Digital Territory concept

By digitising the personal domain but also its boundaries, the Digital Territory concept offers the opportunity to introduce the notion of territory, property and space in a digital environment. The objective is to provide a tool that enables users to manage proximity and distance with others in this future Ambient Intelligence space, both in a legal and a social sense, as we currently do in the physical world.

The physical and traditional concept of residence constitutes a legal sanctuary and protects the citizen from outside interferences or invasive measures[25]. This legal sanctuary has to be now extended to the digital part of our private space.

Communication Challenges

Communication tools will need to be developed in order to express which elements belong to these personal territories.

Links

Beslay, Laurent, Hannu Hakala: Digital Territory: Bubbles. In: Paul T. Kidd (Ed.): European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society, Cheshire Henbury, 2007, pp. 69-78.

Benoliel, Daniel: Law, Geography, and Cyberspace: The Case of online Territorial Privacy, CFP 2004[26]

Daskala, Barbara, Ioannis Maghiros: Digital Territories, Towards the protection of public and private space in a digital and Ambient Intelligence environment[27].

---

[25] *See Articles 7, 8 of the Charter of Fundamental Rights of the European Union*
[26] *See http://www.cfp2004.org/spapers/benoliel-caseOfTerritorialPrivacy.pdf*
[27] *See http://ftp.jrc.es/eur22765en.pdf*