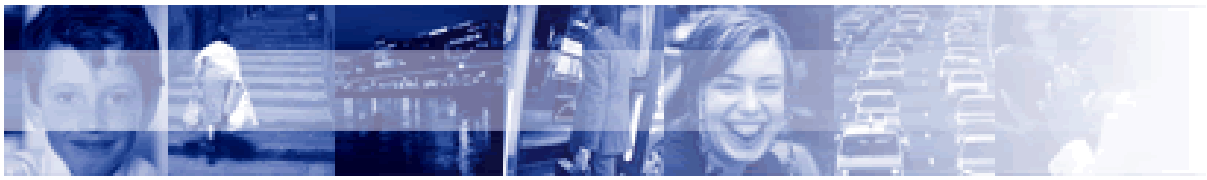
PRISE
privacy • security

Security Research

PASR

Preparatory Action on the enhancement of the European industrial potential in the field of Security research



Grant Agreement no. 108600
Supporting activity acronym: PRISE

Activity full name:
Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

Activity type: Supporting Activity

D 7.3 PRISE Conference Proceedings: "Towards privacy enhancing security technologies – the next steps" Vienna, April 28th and 29th 2008

Final Version, February 2009

Edited by Johann Čas, Institute of Technology Assessment

Supporting Activity Co-ordinator
Johann Čas,
Institute of Technology Assessment, Austrian Academy of Sciences
Strohgasse 45, A-1030 Vienna, Austria
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Partners

Institute of Technology Assessment,
Vienna, Austria
Contact: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

The Danish Board of Technology,
Copenhagen, Denmark
Contact: Lars Klüver
LK@Tekno.dk
www.tekno.dk

The Norwegian Board of Technology,
Oslo, Norway
Contact: Christine Hafskjold
christine.hafskjold@teknologiradet.no
www.teknologiradet.no

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Kiel, Germany
Contact: Marit Hansen
prise@datenschutzzentrum.de
www.datenschutzzentrum.de

Table of Contents **page**

* Abstract or external link

Preface

Over the last years security from crime and terror has become a key issue in public debate and on the political agenda. Many of the proposed measures and technologies meant to increase security are, however, in direct conflict with the human right of privacy. The technical possibilities of surveillance, as well as access to and analysis of personal data are steadily increasing.

A main objective and key result of the PRISE project are criteria for privacy enhancing security research, technologies and measures. Whereas the developed criteria can provide important guidance towards security technologies and measures respecting human rights and personal privacy, they are obviously only a first step to preserve privacy in a security focused world.

The purpose of the PRISE conference was to discuss in an open and broad forum PRISE results as well as further steps required for a balanced approach on privacy and security. The programme was targeted at a broad range of experts on privacy and security issues, representing security industries, policy-making, research, human rights organisations as well as users of security technologies. The aim was to advance public debate and policy discourse and in this way to contribute to security policies in line with human rights and privacy protection.

This deliverable consists of the proceedings of the workshops conducted within the final PRISE Conference, to which the second conference day was devoted. If not indicated otherwise, full text papers are included. Further information on the conference conducted on the 28th and 29th of April 2008 in Vienna is available from the PRISE website http://prise.oeaw.ac.at/, this includes also the presentations of the conference contributions as far as made available to the PRISE project.

The EuropCop project - The impact of the Social, Legal and Ethical aspects in the implementation of ICT dedicated to the pedestrian police officer

Vincent Brochier
Sagem Défense Sécurité
vincent.brochier@sagem.com

Abstract:

Police forces make a major contribution to the security of a country. They protect its frontiers, protect against terrorism and other violence, mange crises – these are the main missions of the police, and all require advances in interoperable integrated systems for information and communication. Lack of progress jeopardises the efficiency of police in the modern world.

The organisation of forces differs from country to country but their **core missions are similar: to protect Life and Property, to prevent Crime, to detect and arrest offenders, to maintain the peace**. The ratio of officers to the public is around 1/1000 in the European Union. Pedestrian police officers will always **be irreplaceable because they have access everywhere (gardens, stairs, cellar…) and they are the front line in any action**. They have to enable lawful activities of all citizens and to protect human rights.

Key to their mission is the ability to gather intelligence, record crime and incidents, retrieve information from police systems and input information into them, identify people encountered, be accessible to their communities. They need to spend as much time as possible engaged in active policing visible to citizens yet be respectful of privacy.

Currently, pedestrian police officers have limited communication equipment and are not included in the police network. Their efficiency suffers from such a situation and globally, they spend only a small part of their time (sometimes as low as 20%) policing on the street; too much of their time is spent in visiting an office or vehicle to access or input information. This directly effects security. There is therefore a strong need to improve the efficiency of pedestrian police officers and in particular to increase the time available for patrol.

Police officers' equipment has to date not been designed in a systemic approach. Potential new equipment has been tested independently in different countries and most of the proposed systems have not been deployed. Various soldiers' equipment programmes (Soldatto del futuro, IZF, F.IS.T, FELIN) explore the future with a systemic approach and can give some ideas of the different types of system and equipment that could be useful for a pedestrian police officer. However the needs and constraints of soldiers and police officers are very different and military equipment can only inspire research not simply be copied for police needs. New ICTs might bring significant improvements, but they could also provide too much information. **At the same time, such equipment can be intrusive because it increases the capabilities of the officer to capture all the information (audio, video) circulating in a public area.** In this case, the reception by the population could be very negative and the efforts made in developing these new technologies could be undermined by fear and the disruption of trust and communication with the populace. **So there is clearly some potential danger to**

provide all these technologies without taking into account the social, legal and ethical implications.

We will present the concept of EuropCop and the process which was undertaken to include these SLE aspects in the technical research process.

Consequently it will demonstrated that EuroCop will integrate new ICT solutions in a suitable way allowing greater efficiency, speed and safety for a police officer in the street while at the same time allowing police officers to be closer to the needs of the citizen without becoming the “henchman” of “Big Brother”.

Balancing the needs for increased security and the protection of fundamental rights in the new generation of video surveillance networks: the example of DYVINE project

Fanny Coudert
Interdisciplinary Center for Law & ICT (ICRI) – Katholieke Universiteit Leuven – IBBT
fanny.coudert@law.kuleuven.be

Abstract:

DYVINE participates from the development of the next generation of video surveillance networks. Video surveillance techniques are evolving from static and passive cameras documenting events to dynamic and preventive networks. The use of wireless IP systems allows the emergence of flexible networks and massive customization at the same time that video content analyses improve their added-value. DYVINE is building a system which will enable few operators to effectively manage complex emergency situations, e.g., creating security perimeters warning against intruders, tracking objects and persons or helping the search for missing people.

This evolution brings however new threats for individual freedoms, challenging in particular the application of the current data protection safeguards. This paper analyses the threats posed by DYVINE system and present the recommendations made within the project to build a system respectful of fundamental rights, pointing out insufficiencies in the protection provided by the legal framework to the new reality of video surveillance capabilities.

1. Introduction

DYVINE (Dynamic Visual Networks) is a European project which deals with the problem of low efficiency of video surveillance systems, despite the growing number of cameras installed in every city, with the aim of enhancing the security and safety of citizens. Nowadays, the main challenge made to video surveillance consists in defining the best way to take advantage of the significant number of streams of images available. The concept of DYVINE is to design a federative system which is able at any time to integrate all the cameras of a city, whoever they belong to, complete them with other cameras, fixed or mobile, in situ or airborne, to provide the risk management agencies with an accurate and up-to-date situation picture of the relevant events. DYVINE-like systems is foreseen to be used during the prevention phase of a crisis and its further management by the Civil Protection agencies and on a permanent basis for Police and Urban management requirements.

DYVINE-like systems are thus called to be used on many different situations with the purpose of enhancing the protection of citizens. Protection should be understood here broadly as referring to ‘the endeavour to preserve human life in the face of both direct (terrorist attacks,

deadly diseases, extreme weather) and indirect threats (risk to the vital systems that sustain human life such as water supplies, electricity provision, health systems and police service)' [1].

This paper deals with the main issues raised by the new generation of video surveillance networks for the protection of citizens from a data protection point of view. Despite being a valuable tool for the police and civil protection forces, several questions should be solved before considering their implementation on a large scale. Such systems should keep an adequate balance between the needs of security and the respect of fundamental rights.

A first part describes the main characteristics of the new video surveillance networks with a particular focus put on the system being developed under DYVINE. This will permit to understand and identify, in a second time, the threats posed by this system to fundamental rights and more particularly how it challenges the safeguards introduced by data protection legislations. Finally, recommendations made within DYVINE to reduce the negative impact on fundamental rights are presented.

2. DYVINE as example of the new generation of video surveillance networks

Video surveillance networks have spread the last decade in response to public security concerns, as a deterrent to crime and for evidence gathering purposes. Other important public interests such as traffic monitoring have also motivated the large deployment of such systems, interweaving a web of video cameras that monitors everyday life of millions of citizens.[2] The efficiency of these systems, i.e. their ability to achieve the goals pursued, is however often put at stake. Suffice is to mention the complaint filed by Privacy International with the Ontario Information and Privacy Commissioner's Office regarding the plans to implement 12,000 cameras across Toronto's transportation network of buses, streetcars, and subways with the goal of crime deterrence.[3] This organisation fundamentally contest the choice of a video surveillance as optimal solution to fight street crime and terrorism, particularly when proof has not been made of its efficiency in this specific domain. They claimed that the benefit for the public good did not seem to justify such interference into fundamental rights. The measure was considered by Privacy International disproportionate and thus lacking of legitimacy.[4]

---

[1] BOIN A., EKENGEN M., RHINARD M., *The European Union's protection policy space: a framework for analysis*, in BOIN A., EKENGEN M., RHINARD M., Protecting the European Union, policies, sectors and institutional solutions, October 2006. As pointed out in this paper., the use of the broad concept of protection instead of the traditional concepts of 'safety', i.e. a term that traditionally covers domestic questions about technological accidents, natural disasters, and other immediate threats to the well-being of citizens, and 'security', a term traditionally related to territorial defense using military means, allows to overcoming the difficulties arising from their blurring both in theory and in practice.

[2] COUDERT, Fanny, DUMORTIER, Jos , *Intelligent video surveillance networks: data protection challenges*, Proceedings of The Third International Conference on Availability, Reliability and Security (ARES'08), 4-7 Mars 2008, IEEE Computer Society, pp. 975-981.

[3] Privacy International, 'PI Files complaint about expansion of CCTV on Toronto transit network', 25 October 2007, available online at: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-558046

[4] The Ontario Information and Privacy Commissioner's Office did however not follow the arguments raised by Privacy International based on the fact that video surveillance systems were not installed and used only for purposes of crime deterrence but also for risk management, public safety, detection and prosecution of crimes. See, Ontario Information and Privacy Commissioner's Office, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report*, Privacy Investigation Report MC07/68, 3 March 2008.

Advances in surveillance technologies are progressively providing tools to remedy the claimed lack of efficiency of video surveillance networks, changing their main nature[5]. Video cameras are not fixed anymore but can adapt their view angle to the needs of the changing circumstances. The use of IP technologies facilitates interconnection and interoperability. Finally, the development of video analytics provides a substantial help in decision-making. These technologies give a new dimension to video surveillance. It evolves from a reactive into a proactive technology, facilitated by the interconnection of networks.[2]

2.1. New video surveillance technologies

New surveillance technologies allow identifying, tracking and investigating diverse activities of formerly anonymous individuals and are fundamentally changing the nature of video surveillance.[5] Three main technological trends can be observed: growing performance of video cameras providing a more precise view of the situation, the use of IP technology which makes video surveillance networks interoperable and finally the use of video analytics tools which improve decision making.

Observation technologies

First of all, video surveillance networks are not fixed anymore, aiming at documenting events in a static way, but make use of sophisticated and re-configurable video cameras that can adapt to the changing needs of a situation. Cameras from closed-circuit television could see about as far as human eye but with a narrower field of view. Modern cameras in contrast can expand their coverage area by panning, i.e. moving in a horizontal plan, tilting, i.e. moving in vertical plan, and magnifying to improve the details that camera images can render. 'With a mere 60-times optical zoom lens a camera can read the wording on a cigarette packet at 100 yards, some cities are reportedly deploying cameras capable of 400-times magnification.'[5] Finally, video cameras can be equipped with night and very low vision thanks to the use of infra-red vision technology.[5]

The growing performance of video cameras certainly expands the possibilities of monitoring public areas in an effective way but at the same time it reduces increasingly the sphere of anonymity enjoyed by individuals in public places.

IP video surveillance networks

Second, video surveillance networks are not 'closed circuits' anymore but tend to be converted in networked digital surveillance based on IP technology. 'IP video surveillance can be defined as the transmission of video utilizing open internet protocols and standards for the purpose of recording and monitoring. This open architecture encouraged third-party software manufacturers to develop management and recording software resulting in exponential growth of the IP video surveillance market'[6].

---

[5] The Constitution Project, Guidelines for public video surveillance, a guide to protecting communities and preserving civil liberties, November 2006, available online at: http://www.constitutionproject.org/

[6] Wikipedia, IP Camera, available online at: http://en.wikipedia.org/wiki/IP_Camera

Apart from reducing costs, IP technology 'supports for a variety of standard and multi-megapixel image resolutions beyond NTSC, PAL and SECAM and the Transmission of commands for PTZ (pan, tilt, zoom) cameras via the same cable'[6], facilitating the integration of networks. It moreover allows the building of federative platforms used by several agencies and the interconnection with third party's networks. The connection of mobile cameras to the network is also facilitated.

The increased flexibility permitted by IP technology enables a growing adaptability of the configuration and characteristics of video surveillance networks to the changing circumstances. It however reduces the transparency of such networks to individuals and contributes to the building of increasingly opaque systems.

Video analytics

Finally, IP technology also supports an increased use of intelligent video analytics tools, namely object recognition software, behaviour analysis and individual and object tracking. The interconnection of video surveillance networks increases their complexity. The spread of video camera networks makes it more difficult to monitor all incoming video feeds. Video analytics provides the necessary help to operators in charge of watching multiple monitors[7]. In that sense, 'computers never loose attention, so video analytics remedies the problem'[7]. But more than the attention required to the operator, it is the ability to analyse the images which is at stake. Video analytics is, according to the definition provided by IBM, 'designed to enable real-time decision-making and post event correlation of people and activities'[8]. It enables 'situation awareness of the location, identity and activity of objects in a monitored space including license plate recognition and face capture'[8].

Embedded intelligent video motion detection with shape recognition/counting applied to objects, people, and vehicles allows increased use of tracking facilities. Integration of video surveillance with other systems and functions such as access control, alarm systems, building management, traffic management, etc allows the design of refined pre-configurable alarms which help to decision-making.[2]

2.2. The example of DYVINE system[9]

DYVINE participates from this new generation of video surveillance networks and integrate these features in order to assist Police and Civil Protection agencies in their daily activities. The system being developed first aims at enabling civil protection forces to work together in view of effectively managing an emergency situation, e.g., creating security perimeters warning against intruders, monitoring the work of firemen or policemen, looking for missing people or tracking objects and individuals and provide them with the required assistance. DYVINE-like systems are however expected to provide powerful tools for local agencies to

---

[7] PANE D., 'Video surveillance networks: Lights, camera, controversy', in Law Enforcement Technology, Officer.com, June 2007, available online at: http://www.officer.com/print/Law-Enforcement-Technology/Video-surveillance-networks--Lights--camera--controversy/1$37805, last accessed on 2nd January 2008).

[8] IBM, Press release, 'IBM unveils new digital video surveillance service', 28 March 2007, available online at: http://www-03.ibm.com/press/us/en/pressrelease/21289.wss, last accessed on 2nd January 2008.

[9] Section based on COUDERT F., VARANGOT G., DYVINE D.5.2. Final version of legal issues, 7 March 2008.

perform several public tasks encompassing public safety, citizen security, traffic management, etc.

The implementation of DYVINE-like systems will typically integrate forests of cameras spread in a city. It will enable access to automatic functions, taking benefit of the videos deployed throughout the city to operators originating from different organisations. Interconnection can also be envisaged at a higher level than the city council in so far DYVINE-like resources can be accessed to by other systems. DYVINE-like system could thus become a valuable tool for other crisis management platforms such as the one developed in various PASR and ESRP projects. The PASR Project MARIUS provides a good example. This project aims to develop a heli-transportable command post for the first reaction after the crisis. As such, the MARIUS Command Post's first task is to assess the situation and damages. It would thus greatly benefit from an enhanced situation awareness picture provided by all the cameras available in the area. In another field (interoperability of law enforcement agencies), the HITS project would also benefit from DYVINE system capability to exchange accurate and real time situation pictures between the agencies in support of the operations.

To that effect, the platform offers a series of specifications:

- *Multi-agencies system*: the platform will support the work of different agencies (firemen, police, civil protection, etc.) with different needs and level of authorization.
- *Interoperability* with other video surveillance systems: the platform is able to interact with other video surveillance systems whenever required in order to provide a better view of the situation
- The system is based on *area processing*: the platform implements processing based on multiple cameras. It allows performing new processing with performances that were not possible on single cameras, e.g. precise location of events.
- The system can support *pre-configurable alarm*: The possibility to integrate smart mobile cameras to the pre-existing networks will allow the dynamic and adaptable configuration of specific alerts depending on the need of the situation. Information is not displayed as such to the operator but in a first time processed and analysed by the local and the intermediary node. The system will thus filter the events on the basis of the pre-defined needs and display only the more relevant information to the operator.
- The system can support *object characterization*: the platform is able to identify relevant objects of surveillance, characterize them in order to allow further data processing, e.g. car or individual tracking.

3. Privacy risks posed by DYVINE-like systems

Despite improving substantially the efficiency of crisis management by Police or Civil Protection forces, DYVINE brings forth considerable risks in terms of fundamental rights. In particular, the connection of several entities at times via an electronic 'centre' may result into recording a considerable amount of personal data and tracking all the passages occurring over a given time span. In that sense, the Working Party 29 have already pointed out that 'the over-proliferation of image acquisition systems in public and private areas should not result in placing unjustified restrictions on citizens' rights and fundamental freedoms; otherwise,

citizens might be actually compelled to undergo disproportionate data collection procedures which would make them massively identifiable in a number of public and private places'.[10]

Data protections legislations play a crucial role in safeguarding fundamental rights against intrusive technologies such as video surveillance. In that sense, the Council of Europe already acknowledged in 1981, when approving the Convention 108 for the protection of individuals with regard to automatic processing of personal data[11], that 'the exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit)'. Indeed, in the field of video surveillance, not only do data protection laws intend to protect the right to privacy, but at the same time, they foresee, e.g., to guarantee the right of movement in an anonymous way or the freedom of expression.

Data protection laws were first enacted in order to prevent abusive interconnections of public databases and to protect individuals from being converted in 'crystal men'. A series of principles have been introduced in order to empower the data subject to keep control over the processing of his/her personal data. However, the interconnection of video surveillance networks puts dramatically at risk those principles, calling for adapted safeguards.

With regard to the prototype being developed under DYVINE, five main privacy risks area have been identified: risks of disproportionate processing of personal data due to the amount of data processed by the system; risks of function creep due to the multi-agency character of the platform; risks of loss of transparency due to the building of an opaque system; risks of abuses due to the use of behaviour analysis tools; and risks of breach of confidentiality of the information processed.

3.1. Excessive collection and processing of personal data.

The main added-value of DYVINE consists in integrating the different video surveillance systems managed by a City in order to provide an overview of the incoming catastrophe. It thus implies the fusion of all the incoming video feeds into a unique processing. The massive personal data processing originated by the integration of video surveillance networks renders the processing highly sensitive, calling for additional safeguards. These video feeds could moreover be enriched by cross-checking the information collected within the network against external databases, e.g. when facial recognition software is being used to identify missing people after an earthquake or wanted people.

[10] Article 29 Data Protection Working Party, 'Opinion 4/2004 on the processing of personal data by means of video surveillance', WP89, 11 February 2004.

[11] Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, ETS n°108, Strasbourg, 28 September 1981.

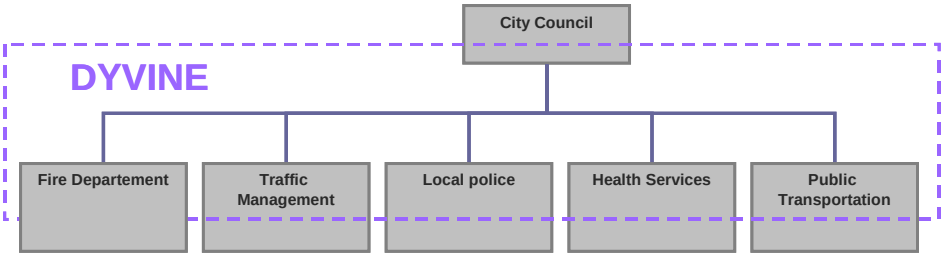


Fig. 1. DYVINE system, a federative video-surveillance system for city council's organizations

© EADS

These features seriously put at stake the proportionality of the processing as it could engender an excessive collection and processing of personal data. The principle of proportionality should guide the balancing of the right to privacy with other competing interests. It grounds the legitimacy of the processing. The monitoring of individuals constitutes by itself a threat to individuals' freedom insofar it seriously reduces their anonymity. The strict application of the proportionality principle in the field of video surveillance is expected to prevent the emergence of pervasive surveillance which could result in an increased vulnerability of individuals.

The deployment of a video surveillance network should be proportionate to the objective foreseen. The principle of proportionality first calls to assess the necessity of the processing carried out. Personal data processing should pass a three-part test and prove that they are able to achieve the goals foreseen (adequacy test) but also be strictly necessary (necessity test), i.e. other processing less intrusive could not be implemented or would prove insufficient, and finally provide sufficient benefits for the public interest to compensate the harm caused to other competing values (strict proportionality test). Due to their highly sensitive nature, video surveillance networks should only be implemented on a subsidiary basis, when the benefits they bring forth for public safety clearly outweigh the increased risks in terms of individual freedoms.

The requirement of proportionality will moreover affects the choice of the most appropriate technology and the filming arrangements applying to the data processing. The visual angles, the possibility of zooming, image-freeze functions, etc. should only be implemented when they are deemed proportionate to the purpose foreseen. In definitive, the use of video surveillance systems should be governed by the principle of minimum intervention.

3.2. The integration of video surveillance networks into a unique processing.

The purpose specification principle compels the controller, i.e. the natural or legal person which determines the purposes and means of the processing of personal data, to collect personal data for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes. This means that the personal data collected can not be processed for purposes beyond the reasonable expectations of the data subject. Further processing can be slightly but never substantially different.

The interconnection of networks implies that, necessarily, the images in first place via the legacy networks will be further processed with a different purpose within DYVINE-like

system, namely the management of an abnormal situation putting at risk the citizens' protection. As the video feeds are merged, it becomes easier to use the data collected for different purposes that the ones originally foreseen. The interconnection of networks thus brings increased risks of function creeps that have to be dealt with.

3.3. The use of advanced software for image analysis increases the risks of interference into individuals' fundamental rights.

Video analytics enables an increased use of automated individual decisions that help decision-making. Automated-based decision systems may be a powerful tool in terms of efficiency of networks but can also bring forth risks of discrimination or put at risks other fundamental rights such as the right to come and go anonymously.

The main concern with regard to automated individual decisions resides in the automatic acceptance of the validity of the decisions reached and a concomitant reduction in the investigatory and decisional responsibilities of humans.[12] In that sense, the Data Protection Directive already contains some safeguards and grants individuals with a right to object to a processing solely based on automated processing and the right to be informed of the logic underlying the decision. This does not however appear sufficient to guarantee a real and efficient protection in opaque system such as the one designed by DYVINE.

Moreover the safeguards ensured by the Data Protection Directive are not applicable to the domain of law enforcement which is mainly regulated by the provisions of the Council of Europe Convention n°108 and the Recommendation R(87) 15 on the use of personal data in the police sector[13] where no reference is made to this specific kind of processing. The Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[14] certainly makes a reference to automated individual decision but let its regulation and thus the balancing of the interests to the appreciation of Member States[15]. This situation seems in contradiction with the growing use of automated decisions, especially in the domain of crime prevention, as illustrated by the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes[16]. The former proposal is moreover still pending and has received heavy criticism for the low level of safeguards it implements.

---

[12] BYGRAVE L.A., Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002.

[13] Council of Europe, Recommendation nº R (87) 15, regulating the use of personal data in the police sector, 17 September 1987.

[14] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ L 350, Vol. 51, 30.12.2008

[15] Article 8 of the decision stipulates that a decision which produces an adverse legal effect for the data subject or seriously affects him and which is based solely on automated data processing for the purposes of assessing individual aspects of the data subject shall be permitted only when the legitimate interests of the data subject are safeguarded *by law.*

[16] Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, COM(2007) 654 final of 06.11.2007.

3.4. DYVINE, an opaque system.

DYVINE-like systems will not directly collect the personal data from the data subjects but will make use of video feeds collected via legacy networks. It thus seems extremely difficult to adequately inform the data subject of the nature of the processing carried out and therefore creates a risk of undermining the level of awareness of the individual with regard to the processing going on.

The transparency principle introduces an obligation of information to the controller to data subjects, prior to the processing of personal data, in addition to granting rights of access, rectification and deletion to data subjects. The main challenge of video surveillance networks, when it comes to transparency, is figuring out the best way to effectively guaranteeing that the data subject is aware of the undergoing processing. So far, the solution has consisted in compelling the controller to place an information notice in visible places. However, this remains unsatisfactory and insufficient. Individuals should be aware of the fact that their personal data are being processed, for which purposes and who is carrying it out. This enables them to exercise their rights of access, objection and deletion.

DYVINE is building a fundamentally opaque system. It illustrates the difficulties of traditional means in ensuring the transparency of interconnected networks and systems. Such systems do not offer a direct interaction with the data subject for one part, and do not collect information directly from the data subject. Alternative transparency tools should be devised for these systems.

3.5. Confidentiality of the information processed.

The massive processing of video images originating by the use of DYVINE systems renders security measures of significant importance. The integration of the video surveillance networks could indeed lead to a centralization of the personal data to be recorded even if they proceed from different processing. This increases significantly the risks of security breach and of function creep. Furthermore, the use of wireless communications by DYVINE increases the risks of intrusion in the system. Eavesdropping and intrusion are easier as the signal is sent over the air and no physical connexion is required.

4. Reconciliating security with privacy.

DYVINE-like systems, if they are to be generalized, should not only take into account the current legal constraints but to develop a socially acceptable solution in terms of civil liberties and the fundamental right to privacy. The difficulty resides in the fact that the systems can consequently be used on different “modes” with distinct functions: on a ‘day-to-day’ basis the system would serve the specific purposes of each network; when a natural or man-made catastrophe occurs it could be used the management of the crisis; and finally when circumstances justify it, the system could be used for public safety purposes. It is thus absolutely necessary that the required safeguards are adaptable and implemented in such a way as to adequately answer the needs of all three situations. To that effect, several recommendations have been made tending on the one hand to integrate privacy safeguards in

the design of the system, and on the other hand to adapt the current legal safeguards to the specific risks posed by these systems.

4.1. Privacy by design

A series of recommendations has first been made in order to build privacy concerns right into the design of the system. What is intended here is to prevent unwanted accident by limiting the possibility of misuse or abuse.

DYVINE as dormant system

First, in order to limit the cases where the video feeds are merged, the system is recommended to be conceived as a '*dormant system*'. This means that the merge of legacy video surveillance networks should exclusively be activated when a series of predefined conditions ensuring the lawfulness and legitimacy of DYVINE processing occurs. On a daily basis, the system is not apparent to the user who can only access the data he is entitled to, extracted from the video surveillance network he usually uses. In case of emergency or any other event that could justify the use of DYVINE-like system actively, the system is activated and the user will gain access to the images he needs to perform his task.

Strict definition of access rights

In order to ensure that each user obtain access only to the images he needs for the performance of his task, a strict definition of *users' access profiles* should be implemented. As a way of example, a police officer could use some of the tracking functions whereas these functions would not be made available for a health service operator.[9]

Moreover, the consulted video images and the results of each processing are to be accessed according to users' rights. The rights are checked whenever a user accesses the video, data and processing, and a correct filtering is performed corresponding to the user rights. As an example, a traffic regulator operator could see detailed information concerning vehicles, whereas third party operator could see only general information. The exchange of information between organisations is subject to the same filtering on data.[9] In addition, digital water markers help creating a clear record of where and when records were accessed.

The figure below represents a first general architecture of DYVINE system, considering the recommendations relative to legitimacy, proportionality and data minimisation principle.

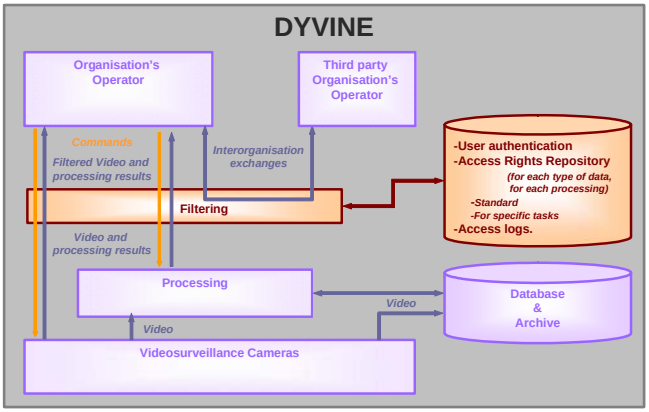


Fig. 2. Functional architecture of the logical access function of DYVINE system, © EADS

The use of pre-configurable alarms as data minimization tool

The use of *pre-configurable alarms* is advocated in order to reduce the amount of data to be displayed on the screens to the information strictly necessary. These alarms would lead to display exclusively the images related to abnormal events or behaviours to be detected by the system. The definition of configurable alarms function of the events and thus the fact that the system (via the local and intermediary node) is able to determine the data that should be accessed to by the operator may be a first step into the designing of less privacy-intrusive video surveillance networks. The operator does not need to watch the whole footage in order to take a decision but he is alerted by the automatic video surveillance system whenever an event identified as worth of attention occurs.

This solution is also advocated by the UK Royal Academy of Engineering. In the report on 'Dilemmas of Privacy and surveillance'[17], this academy proposes 'to devise systems that only stepped into action when a suspected crime was taking place. Instead of having operatives scanning hours of mundane footage, feed from the cameras could be examined by an automated system, which alerted the operative when suspicious activities were detected. This would mean that ordinary activities would be effectively ignored, and certainly not scrutinized by an operative.' In that sense, it is argued that 'if a system is developed that can successfully target only suspicious behaviour, the law-abiding citizen can be confident that their behaviour is not under scrutiny. Furthermore, research shows that stereotypes seem to affect the way that CCTV operators monitor footage, meaning that surveillance systems have a more negative effect on those who tend to receive poorer treatment in other areas of life. Automated surveillance systems could instead be programmed on the basis of fact rather than prejudice.' [17]

An automatic video surveillance system which would display only the sequences related to abnormal events may indeed reduce the intrusion into privacy as well as raising the efficiency of the use of video surveillance systems. This does not mean that the mere filming of public spaces, even when no alert is raised would fall outside the scope of application of data protection laws or that the use of such alert would always be in conformity with their provisions. On the contrary, it should be seen as a double-edged sword and should be carefully

[17] The Royal Academy of Engineering, Dilemmas of Privacy and Surveillance, Challenges of technical changes, March 2007, available online at: http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf

considered in so far the nature of some alerts such as the ones based on human behaviour analysis may result highly intrusive.

Decentralization of the information stored

Finally, the integration of the video surveillance networks could indeed lead to a centralization of the personal data to be recorded even if they proceed from different processing. The centralization of data increases the risks of security breach and of function creep and should be avoided as far as possible. Alternative solutions such as the storage of the data in separated databases corresponding to each legacy video surveillance network should be preferred.

4.2. Better use of existing measures: an increased use of the prior checking procedure and of Privacy Impact Assessments

Finally, the risks posed to privacy, in particular the difficult assessment of proportionality, call for a growing implication of Data Protection Authorities, in particular via the prior checking procedure. These procedures are directed to examine processing operations likely to present specific risks to the rights and freedoms of data subjects, before they start. The Data Protection Authority may, according to its national law, give an opinion or an authorization regarding the processing (Recital 54 of the Data Protection Directive). The Data Protection Directive however let to Member States the choice whether to implement these procedures and the processing object of such procedure. This has resulted in a very scarce use of the procedure in practice. It is however progressively implemented in some countries. As a way of example, in France, prior checking is mandatory for processing involving biometrics, the same procedure is however voluntary in Italy but can also be used for video surveillance processing.

The threats posed by DYVINE-like systems to privacy as described in this paper call for prior check of such systems by Data Protection Authorities. These authorities would be able to ensure that the system is compliant with data protection principles, in particular with the principle of proportionality, an operation that cannot be let to the sole controller.

In addition and to prepare the prior checking procedure, controllers should systematically carry out a Privacy Impact Assessment (PIAs). PIAs allow the controller to identify and manage privacy risks prior to the implementation of a system. In order to define the purposes and assess their legitimacy, the Information Commissioner Office (UK Data Protection Authority) – and the Data Protection Authority of Madrid for video surveillance processing- are already recommending that organisations carry out PIAs before starting any new projects or programmes that may have privacy implications. The Information Commission Office considers that by performing a PIA at an early stage of a project, organisations can identify any problems before it is too late. These PIAs should moreover have a follow-up with the objective to assess whether the processing is having the desired effect, for example in terms of reducing crime or providing a more efficient service to the public.[18]

[18] For more information on Privacy Impact Assessments as advocated by the UK DPA, see the dedicated web page of this body at: http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_conference.aspx

4.3. Unsolved problems: new safeguards required

The development of fundamentally opaque systems making use of video analytics tools raise new privacy concerns that require not only the implementation of technical and organizational safeguards but also a modification of the legislation. Two areas are specially focused on: the needs to enhance the protection against automated individual decision and to devise new transparency tools that re-establish the equilibrium between 'watchers' and 'watched'.

Individual tracking and behaviour analysis: ensuring a better protection against automated individuals decisions[19]

An increased used of video analytics renders individuals more exposed to automatic individual decision. It facilitates tracking or behavior analysis that can be by itself subject to specific safeguards, e.g. the obtaining of a warrant when performed by police for law enforcement purposes, or that can result in harmful consequences for the individuals, e.g. discriminatory practices. As mentioned above, article 15 of the Data Protection Directive had tried to tackle the issue of increased automation in the decision-making process, mainly with regard to organizational decisions. Article 15 aims at protecting 'the interest of the data subject in participating in the making of decisions which are of importance to him.' The use of extensive data profiles of individuals by powerful public and private institutions was seen as risking to 'deprive the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadows''[12]. The problem of the lack of transparency was already at the centre of the debate.

A second fear which was expressed in the debates surrounding Data Protection Directive was that 'the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities'[20]

As highlighted by Bygrave 'the increasing automation of decision-making processes engenders automatic acceptance of the validity of the decisions reached and a concomitant reduction in the investigatory and decisional responsibilities of humans. Thus, there is an implicit assumption that the reasoning linking the premises and conclusions for these predictive judgments will be grounded in reality.' [12]

Another problem arises with regard to the opacity of the algorithms used which are not necessarily connected to truisms about human behaviour. As stressed by Steinbock, contrary to human judgment, 'computer analysis has no way to evaluate the probable accuracy of the data on which it relies'[21]. In addition, computer reasoning is more difficult to evaluate than human assessment.

This situation let the individual relatively unprotected against automatic individual decisions which could result in harmful consequence. The time may have come to rethink the safeguards designed to grant the data subject with sufficient protection and in particular, to provide him with adequate tool to defend himself in an efficient way. In any case, in the field of law

---

[19] This section is based on considerations issued in Coudert F., De Vries E., Kowalewski J., *Legal implications of forensic profiling: of good old data protection legislation and novel legal safeguards for due processing*, in FIDIS D.6.7. Forensic Profiling, not published yet.

[20] COM(90)314 final - SYN 287, 13 September 1990, p. 29.

[21] STEINBOCK, D., *Data Matching, Data Mining, and Due Process.* Georgia Law Review 40(1): 1-84, 2005.

enforcement, traditional safeguards as contained in criminal law, in particular surrounding the tracking of individuals, remain applicable.

Once again, the needs of law enforcement activities will need to be balanced with individuals' rights. Prior safeguards, such as a strict assessment of the conditions required for the legitimacy of such processing, may be needed. Intervention of independent authorities may be required as well in order to restore the equilibrium between watchers and watched.

New mechanisms of accountability to be devised

The building of opaque systems such as the one of DYVINE endangers the objective of data protection systems to put the individual at the centre of the mechanisms installed, to provide him with specific instruments to manage the control over the processing of his data by himself, and thus to make the processing transparent to the data subject. Several scholars have pointed out this phenomenon where 'individuals becomes each time more transparent and heteronomous in the construction of their personality, whereas private and public institutions become each time more opaque and invest on 'autonomy' and 'automatisms' in the construction of the mode of intelligibility, interpretation and reaction towards individuals'[22]

Transparency needs to be guaranteed by alternative mechanisms, such as the intervention of external independent authorities, e.g. the Data protection Authorities, monitoring the correct application of legal safeguards. In that sense, the French Data Protection Authority has recently pointed out the fact that 'the question of the control of video surveillance system by an independent authority, in other words, 'the control of the controllers', from now on forms a fundamental requirement in modern democratic societies, necessary to ground the legitimacy of the development of systems ensuring the implementation of safeguards that take into account the rights and liberties of individuals.'[23]

Other forms of transparency safeguards should be envisioned. These new tools for transparency not only will have to give the power back to the citizens over the processing of his data but also to ensure the accountability of the controller. Without proper accountable safeguards that deter, detect and punish misuse or abuse of the system, controllers may never have to explain their actions.[5]

5. Conclusion: how to ensure an effective protection within the second generation of video surveillance networks?

Recent advances in video surveillance technologies are seriously challenging the efficiency of our current data protection safeguards. Massive collection of personal data, merge of systems and networks, increased capabilities of systems in terms of analysis of images increase the risks of excessive processing of personal data in the name of security. 'Public video surveillance systems pose new and more serious threats to constitutional rights and valued than the surveillance cameras in the past. Existing laws and regulatory proposals are insufficient to adequately cope with these threats.'[5]

---

[22] A. ROUVRAY, *Repenser le sens du droit à la protection de la vie privée dans la société de surveillance : une urgence démocratique*, Proceedings of the Juritic Seminar on *La vidéo surveillance : quel équilibre entre sécurité et protection de la vie privée* , Namur (Belgium), 18 January 2008.

[23] CNIL, Press release, Vidéosurveillance : la CNIL demande un contrôle independent, 8 April 2008, available online at: http://www.cnil.fr/index.php?id=2413

In order to prevent slipping into a society where privacy would be sacrificed to the needs of security, we advocate for a three step approach. First of all, technical safeguards that would prevent or at least limit the risks of abuse of the system should be integrated into its design. Second, greater implication of Data Protection Authorities in the control of the 'watchers' in order to ensure a strict application of the principle of proportionality should be considered. These authorities have acquired a significant experience in safeguarding individual rights in the field of new technologies throughout the years and have been granted with sufficient independency and autonomy as to be able to generate the sufficient trust amongst citizens. Finally, new legal safeguards may be required in particular when it comes to the protection of individuals against automated individual decisions and ensuring the accountability of the watcher. The new systems have characteristics which can only insufficiently be apprehended by the current legislations and may need a specific answer.

Acknowledgements

This work has been funded by the European Commission FP6 Framework Programme through the Integrated Project DYVINE. The author would like to thank Guilhem Varangot and Philippe Chrobocinski for their support with technical knowledge and their critical review of the solutions proposed.

Technological trends in screening and security measures

Anne Kets
Rathenau Institute
a.kets@rathenau.nl

Abstract:

Within the last decennium a large number of security measures came into effect within the Netherlands, possibly changing the Netherlands from a privacy minded country towards a more security minded society.

The measures that came into effect range from legislation allowing policy, judiciary and security services to link files and databases and obtain data from third parties for security purposes, to the increased use of security cameras within the public area. The trend towards the increased use of security measures, however aggravated by the 9/11 attacks and the murder on Dutch film director Theo van Gogh in 2004, started before September 2001. The measures have been introduced without much public discussion. Moreover, the discussion that occurred focused on effects of specific measures, not on the accumulated privacy effect of the security measures taken together. The discussions furthermore mostly occurred within closed legal circles and scarcely focused on the privacy of ordinary citizens.

The lack of public discussion also arose from the lack of agitation within the public. Public opinion polls show that citizens however valuing their privacy, value their security over it. A number of citizens even support the phrase that governments may know everything about them as they have nothing to hide. It seems that citizens generally trust their government that security measures are both necessary and effective.

However one could wonder whether ordinary citizens are sufficiently informed about the possible positive and negative effects of the accumulation of measures in place. The effectiveness of most measures is unknown. Also little is known about the effects of likely future developments. The effects of for instance a new citizens number, to be used in all public and semi private sectors, the use of a RFID chip system for public transport, and the introduction of biometric passports are unclear especially within the context of other measures already taken.

One more general and recent trend in the fight against crime and terrorism is that research increasingly has a exploratory character. Potential suspect groups are monitored based on risk profiles. The data load increases, intelligence service increasingly have access to information from other government and semi private services. The use of new technologies will increase the availability of data available, the quality of data is however not always clear.

Due to the increased availability of data, the services can collect even more information on suspects *and* ordinary citizens than ever before. This may have negative effects on the privacy and civil rights of ordinary citizens. These developments raise questions about the efficiency of data collection on suspects and non suspects alike. Does the increased availability of data make it easier or harder to find the pin in the haystack? Are data always right? Another issue is

the legal protection of possible innocent persons that come to the services' attention. How does someone become a suspect and is it possible to prove one's innocence?

In order to further investigate possible technological mechanisms behind the increased application of technological options for security purposes we have focused on the introduction and use of three technologies: the use of DNA material in forensics, the use of data systems for intelligence and surveillance' purposes and the use of surveillance cameras.

For each of these technologies we have made an overview of developments in the Netherlands within a European perspective. The overview describes the options' possible effects on the privacy and security of ordinary citizens, other possible side effects and bottlenecks in the efficient and just use of these technologies. Here issues arise as the continuous increase in use of these three technologies, the possibility of false positive results when data mining, possible interpretation errors in the use of DNA material in court and the uncertain effects of surveillance cameras in fighting crime or even in letting people feel more secure.

The outcomes of these three cases are used to draw more general conclusions on technological trends that possibly underlie the increasing use of surveillance technologies in the Netherlands. The hypothesis here is that governments place too much trust in surveillance technologies and a stronger legal framework better enabling citizens to defend themselves is needed. The overview forms the input for an expert meeting on digital security in March 2008. In this meeting with politicians and experts conclusions will be drawn about the possible political consequences of these technological trends in a broader perspective.

Privacy issues coverage in the 3DFace project

Mario Savastano
IBB - CNR (National Research Council of Italy)
Mario.savastano@unina.it

Abstract:

How privacy issues have been approached in a EC funded Integrated Project concerning biometric technologies

"3DFace" is an Integrated Project of FP6 clearly focused on 3D face recognition technology research, including fusion with 2D face recognition technologies, and its application in secure environments. The project follows the approach of exploiting the rich feature space provided by the geometry of the face surface aiming to increase reliability in self-service border controls.

An important focus of the project involves privacy issues, both in enabling a robust protection of the 3D biometric templates and for approaching all the cross-jurisdictional issues connected to the protection of personal data. Since the start of the project, a specific WP is taking care of such cross-jurisdictional aspects.

The aim of the proposed presentation will highlight the activity carried out in the WP with special reference to a website specifically created for supporting the experts in approaching the cross-jurisdictional issues connected to the project.

The website should be opened to the 3DFace experts in the month of April 2008 and then, successively, most likely, to the general public. The website, other to particular features for giving answers to specific question raised by the 3DFace project members, contains a repository of documents pertaining to cross-jurisdictional issues and biometrics collected not only in Europe but also in several other countries such as Japan, Australia and New Zealand.

Privacy Impact Assessments: What are they and how can they be made to work?

Colin Bennett
Department of Political Science at the University of Victoria, Canada
cjb@uvic.ca

The presentation of Colin Bennett was based on the results from the „Privacy Impact Assessment Project", a study into the use of Privacy Impact Assessments (PIAs) around the world, commissioned by the ICO, the Information Commissioner's Office of the UK (http://www.ico.gov.uk/). Coordinated by the University of Loughborough, this groundbreaking work looked at the use of PIAs in other countries, identified the lessons to be learned from their experiences and developed a PIA methodology for use in the UK. This study is available at http://www.ico.gov.uk/Home/about_us/research/data_protection.aspx.

Biometrics – how to put to use and how not at all?

Andreas Pfitzmann
Computer Science Department of Dresden University of Technology, Germany
Andreas.Pfitzmann@tu-dresden.de

How to handle security problems of biometrics and how to handle security and privacy problems caused by biometrics

Biometrics is advocated as *the* solution to admission control nowadays. But what can biometrics achieve, what not, and which tasks in system design does this pose?

What is Biometrics?

Measuring physiological or behavioral characteristics of persons is called biometrics.

Measured are, e.g., the *physiological characteristics*

- (Shape of) Face,
- Facial thermograms,
- Fingerprint,
- Hand geometry,
- Vein patterns of the retina,
- Patterns of the iris, and
- DNA

or, e.g., the *behavioral characteristics*

- Dynamics of handwriting (e.g. handwritten signatures),
- Voice print, and
- Gait.

One might make a distinction whether the person, whose physiological or behavioral characteristics are measured, has to participate explicitly (*active* biometrics), so (s)he gets notice that a measurement takes place, or whether his/her explicit participation is not necessary (*passive* biometrics), so (s)he might get no notice that a measurement takes place.

Biometrics for what Purpose?

Physiological or behavioral characteristics are measured and compared with reference values to

- *authenticate* (Is this the person (s)he claims to be?)

or even to

- *identify* (Who is this person?).

Both decision problems are the more difficult the larger the set of persons, of which persons have to be authenticated or even identified. Particularly in the case of identification, the precision of the decision degrades with the number of possible persons drastically.

Security Problems of Biometrics

As with all decision problems, with biometric authentication/identification, two kinds of failures occur:

- Persons are wrongly not authenticated or wrongly not identified.
- Persons are wrongly authenticated or wrongly identified.

This leads to the dilemma of (biometric) pattern recognition [3]: If the similarity test is strict, people will be wrongly accepted or identified only rarely – but wrong non-acceptance and non-identification will happen more often. If the similarity test is less strict, people will be not accepted or not identified only rarely – but wrong acceptance and wrong identification will happen more often.

Practical experience has shown that only the frequency of one error type can be kept small – and the price to be paid for that is that the frequency of the other error type increases.

A biometric technique is more secure for a certain application area than another biometric technique if both error types occur more rarely. It is possible to slightly adapt the strictness of similarity tests used in biometrics to various application areas. But if only one of the two error rates should be minimized to a level that can be provided by well managed authentication and identification systems that are based on people's knowledge (e.g., passphrase) or possession (e.g., chip card) today's biometric techniques can only provide an unacceptably high error rate for the other error rate.

Since more than two decades we hear announcements that biometric research will change this within two years or within four years at the latest. In the meantime, I doubt whether such a biometric technique exists, if the additional features promised by advocates of biometrics shall be provided as well:

- user-friendliness, which limits the quality of data available to pattern recognition and
- acceptable costs despite possible attackers who profit from technical progress as well (see below).

In addition to this decision problem being an inherent security problem of biometrics, the implementation of biometric authentication/identification has to make sure the biometric data come from the person at the time of verification and are neither replayed in time nor relayed in space [5]. This may be more difficult than it sounds, but it is a common problem of all authentication/identification mechanisms.

Security Problems caused by Biometrics

Biometrics does not only have the security problems sketched above, but biometrics' use also causes security problems. Examples are given in the following.

Devaluation of classic forensic techniques

Widespread use of biometrics can devaluate classic forensic techniques as sketched for the example of fingerprints as a means to trace people and provide evidence:

- Databases of fingerprints or common issuing of one's fingerprint essentially ease the fabrication of finger replicas and thus leaving someone else's fingerprints at the site of crime.
- If biometrics employing fingerprints is used to secure huge values, quite probably, an "industry" fabricating replicas of fingers will arise.
- As infrastructures, e.g. for border control, cannot be upgraded as fast as single machines (in the hands of the attackers) to fabricate replicas of fingers, a loss of security is to be expected overall.

Stealing body parts (Safety problem of biometrics)

In the press you could read that one finger of the driver of an S-class Mercedes has been cut off to steal his car. Whether this story is true or not, it does exemplify a problem I call the safety problem of biometrics:

- Even a temporary (or only assumed) improvement of "security" by biometrics is not necessarily an advance, but endangers physical integrity of persons.
- If checking that the body part measured biometrically is still alive really works, kidnapping and blackmailing will replace the stealing of body parts.

Wanted multiple identities could be uncovered as well

The naive dream of politicians dealing with public safety to recognize or even identify people by biometrics non-ambiguously will become a nightmare if we do not completely ignore that in our societies accepted and often useful multiple identities for agents of secret services, undercover agents and persons in witness-protection programs do and have to exist.

The effects of a widespread use of biometrics would be:

- To help uncover agents of secret services, each country will set up person-related biometric databases at least for all "foreign" citizens.
- To help uncover undercover agents and persons in witness-protection programs, in particular organized crime will set up person-related biometric databases.

Whoever believes in the success of biometric authentication and identification, should *not* employ it on a large scale, e.g., in passports.

Privacy Problems caused by Biometrics

Biometrics is not only causing security problems, but privacy problems as well:

- Each biometric measurement contains potentially sensitive personal data, e.g. a retina scan reveals information on consumption of alcohol during the last two days, and it is under discussion, whether fingerprints reveal data on homosexuality [2; 1].
- Some biometric measurements might take place (passive biometrics) without the data subject getting to know of it, e.g. (shape of) face recognition.

In practice, the security problems of biometrics will exacerbate their privacy problems:

- Employing several kinds of biometrics in parallel to cope with the insecurity of each single kind [6], multiplies the privacy problems (cf. mosaic theory of data protection).

Please take note of the principle that data protection by erasing personal data does not work on the Internet, since it is necessary to erase *all* copies. Therefore even the possibility to gather personal data has to be avoided. This means: no biometric measurement.

How to put to Use and how not at all?

Especially because biometrics has security problems itself and additionally can cause security and privacy problems, one has to ask the question how biometrics should be used and how it should not be used at all.

Between data subject and his/her devices

Even biometric techniques that often accept people erroneously, but rarely reject people erroneously, can be used between a human being and his/her personal devices. This is even true if they were too insecure to be used in other applications or would cause severe privacy or security problems in these other applications:

- Authentication by possession and/or knowledge and biometrics improves security of authentication.
- No devaluation of classic forensic techniques, since the biometric measurements by no means leave the device of the person and persons are not conditioned to divulge biometric features to “foreign” devices.
- No privacy problems caused by biometrics, since each person (hopefully) is and stays in control of his devices.
- The safety problem remains unchanged. But if a possibility to switch off biometrics completely and forever after successful biometric authentication is provided and this is well known to everybody, then biometrics does not endanger physical integrity of persons, if users are willing to cooperate with determined attackers. Depending on the application context of biometrics, compromises between no possibility at all to disable biometrics and the possibility to completely and permanently disable biometrics might be appropriate.

How not at all?

Regrettably, it is to be expected that it will be tried to employ biometrics in other ways:

- Active biometrics in passports and/or towards “foreign” devices is noted by the person. This should help him/her to avoid active biometrics.
- Passive biometrics by “foreign” devices cannot be prevented by the persons themselves – regrettably. Therefore, at least *covertly employed passive biometrics should be forbidden by law*.

What does this mean in a world where several countries with different law systems and security interests (and usually with no regard of foreigner’s privacy) accept entry of foreigners into their country only if the foreigner’s country issued a passport with machine readable and testable digital biometric data or the foreigner holds a visa containing such data?

Visas including biometrics or passports including biometrics?

Visas including biometrics do much less endanger privacy than passports including biometrics.

- Foreign countries will try to build up person-related biometric databases of visitors – we should not ease it for them by conditioning our citizens to accept biometrics nor should we make it cheaper for them by making our passports machine readable.
- Organized crime will try to build up person-related biometric databases – we should not ease it for them by establishing it as common practice to deliver biometric data to "foreign" machines, nor should we help them by making our passports machine readable without keeping the passport holder in control (cf. insecurity of RFID-chips against unauthorized reading, http://dud.inf.tu-dresden.de/literatur/ Duesseldorf2005.10.27Biometrics.pdf).
- Since biometric identification is all but perfect, different measurements and thereby different values of biometric characteristics are less suited to become a universal personal identifier than a digital reference value constant for 10 years in your passport. Of course this only holds if these different values of biometric characteristics are not always "accompanied" by a constant universal personal identifier like the number of your passport.

Outlook

Like the use of every security mechanism, the use of biometrics needs circumspection and possibly utmost caution. In any case, in democratic countries the widespread use of biometrics in passports needs a qualified and manifold debate. This debate took place at most to some extent and unfortunately, it is not encouraged by politicians dealing with domestic security within the western countries, but they even refused it or – if this has not been possible – manipulated the debate by making indefensible promises or giving biased information.

This text shows embezzled or unknown arguments regarding biometrics und tries to contribute to a qualified and manifold debate on the use of biometrics.

After a discussion on how to balance domestic security and privacy, an investigation of authentication and identification infrastructures [4] that are able to implement this balance should start:

- Balancing surveillance and privacy should not only happen concerning single applications (e.g. telephony, e-mail, payment systems, remote video monitoring), but across applications.
- Genome databases will possibly undermine the security of biometrics measuring inherited physiological characteristics.
- Genome databases and ubiquitous computing (= pervasive computing = computers in all physical things connected to a network) will undermine privacy primarily in the physical world.
- Privacy spaces in the digital world are possible (and probably needed) and should be established – instead of trying to gather and store traffic data for a longer period of time at high costs and for (very) limited use (in the sense of balancing across applications).

References

1. Forastieri, V. Evidence against a Relationship between Dermatoglyphic Asymmetry and Male Sexual Orientation; *Human Biology* 74/6 (2002) 861-870.

2. Hall, J. A. Y. and Kimura, D. Dermatoglyphic Asymmetry and Sexual Orientation in Men; *Behavioral Neuroscience*, 108 (1994) 1203-1206. www.sfu.ca/~dkimura/articles/derm.htm

3. Jain, A., Hong, L. and Pankanti, S. Biometric Identification; *Communications of the ACM* 43/2 (2000) 91-98.

4. Pfitzmann, A. Wird Biometrie die IT-Sicherheitsdebatte vor neue Herausforderungen stellen? DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 29/5 (2005) 286-289.

5. Schneier, B. The Uses and Abuses of Biometrics; *Communications of the ACM* 42/8 (1999) 136.

6. Ross, A. A., Nandakumar, K., and Jain, A. K. *Handbook of Multibiometrics*, Springer, New York, 2006.

Towards New Design Practices for Security Technologies?

Leon Hempel
Center Technology and Society, TU Berlin
hempel@ztg.tu-berlin.de

Abstract:

Security regimes aim to cope with the complexities and inconsistencies of the social world in diverse settings. With the rapid development of information and communication technologies systems have become increasingly hybrid, combining human and technological agency distributed over space, time, diverse actors and institutions and thus characterized by multifaceted interactions. The continuous trend, for instance, towards further automatisation of organisational work processes in these regimes implies that humans and technological devices increasingly interact beyond delegation from humans to machines, on a small scale in facial recognition systems on a large scale in electronic data processing and positioning systems. The interactions occur on an equitable level between human and technological partners in a multilateral coordination context. This immediately raises the question and ethical concern: to whose competences system interventions in critical situations, infringements to privacy and violations of human rights and social values can actually and finally be attributed to?

Due to an increase competence and autonomy of the technological devices it may become difficult to decide whether the interaction partner is human or artificial or both. We witness a situation of widespread ‘surveillance assemblages’, organisationally decentralized and centralized, connecting manifold civil and military uses. Large system integration (LSI), as the industry calls it, targets to meet surveillance and security tasks including compound security, trafficking of illegal goods, safety monitoring and evacuation on a 24h/7 days basis. The goal is to include the integration of sensor technologies, data fusion and intelligent observation systems to enable stand-off detection and analysis through barriers, of substances, of carriers and people as well as behaviour analysis to separate potential perpetrators from crowds, to neutralise threats and so on and so forth.

Being 'mixed initiative systems', ‘regulative’ or ‘interventional’ approaches that aim not only to unravel social and ethical implications but seek to provide new possibilities to limit identified individual and social risks from the beginning are needed. However, taking a closer look on innovation journeys and contexts of individual technologies these are strongly confronted with opposing challenges that limit chances to intervene to a minimum. In my paper I therefore want to follow the path of several approaches by focusing at the same time on these specific challenges with in technical innovation in more detail. As starting point, I will concentrate on standard evaluations and traditional Technology Assessments (TA) confronting their naïf normativism with the proliferation of CCTV in the UK. I will show how technological promises in combination with the implementing of technologies leads to the (present and) very uncomfortable situation of loosing control in regard to everyday deployments. The questions of requirements is either completely forgotten or simply negatively addressed by those - such as police staff - experiencing that the technology does simply not work in the way it has been promised in the first place.

Looking first at Privacy Impact Assessment (PIA) and its recent efforts I will shortly discuss the necessity to connect Privacy with Science and Technology Studies (STS) before I than will present and discuss an approach that is originated in STS, known as Constructive Technology Assessment (CTA) and that offers a direction in my opinion worth to consider for the privacy-security-dilemma. Invented by Arie Rip and Johan Schot in the Netherlands, CTA aims to shift "the focus away from assessing impacts of new technologies to broadening design, development, and implementation processes." It stresses that "promotion actors (engineers and others) need to realize that when they are engineering technology they are also engineering society."

Accordingly, CTA demands multidisciplinary approaches for technological design processes. There are at least three particular CTA strategies I will present in respect to the privacy/security-dilemma in detail: technology forcing, strategic niche management and alignment that has its precondition in the identification of loci within the technology development for reflexivity and learning. Whether CTA can help to overcome the existing conflict between security requirements and the need to protect privacy and civil rights has to be tested. However, its advantage lays first of all in its understanding that technology design is a social and thus open process.

Privacy by Design. The "Whole System" Approach

Andrew A. Adams
School of Systems Engineering, University of Reading
a.a.adams@reading.ac.uk

Abstract:

In the eighties the requirements analysis and system design of computer and communications technology focussed first and foremost on the internal technical elements. The interface design, whether that interface was to a human being or a separate hardware or software system, was a late, underfunded addition to the system. That has changed and various design methods put the interface of the system at the core of the requirements analysis and design phases of a project. Certainly the expected and possible future use of systems is part of good project management.

In the Information Age, computer and communication technology invades all elements of life and increasingly law enforcement, public order, safety and anti-terrorism activities rely on a wide variety of technology. In some cases one particular technology has seen wide scale adoption without significant consideration of the impact on the lives and hitherto expected freedoms of ordinary citizens. The rapid expansion of CCTV in the UK in the nineties is now the classic example [NA99].

One of the difficulties posed in this area is the disjunction between the bearer of the cost and the beneficiaries of the benefits in the design and deployment of security technology. The UK's "sleepwalk into a surveillance state" [Com06] was caused not by deliberate malice, prurient interest or a lack of personal ethics on behalf of the policemen, politicians and civil servants engaged in CCTV and database deployments in the UK. It was driven by a lack of good frameworks for including privacy "costs" (and other negative ethical consequences) in design and deployment decisions for security technology.

Learning the lessons from the earlier usability crisis, and from the field of environmental protection, the UK's Information Commissioner's Office commissioned the development of the Privacy Impact Assessment (PIA) Handbook [Com07], based on earlier work in Canada, Australia and New Zealand. The obvious parallels with the now well-established Environmental Impact Assessment process give assurance that this can be a very useful tool for the ethical engineer and decision-maker to work with in taking into account the potential negative consequences of particular elements of a security technology's design.

Good as the PIA approach is, it is still incomplete. For, while engineers designing security technology, working with ethical and legal experts, may make appropriate technology selections by including privacy enhancing tools as part of a design, or by deliberately not including certain technological capabilities in a system, there remain some significant issues which require continued attention to the ethical (and particularly the privacy) implications of security technology beyond the system design and implementation phases.

The Misuse Question Designers, manufacturers and distributors of security technology1need to be aware that not all those purchasing their products will necessarily be honest and

ethical. Both during a PIA process, and in the regulation of sales of systems, the potential for misuse must always be taken into account.

The Abuse Question Even where the organisation purchasing and deploying security technology have appropriate ethical approaches, not all of their employees may be so honest. The well-documented tendency of CCTV operators to abuse their position for voyeuristic sexual thrills[NA99, p. 129] is an obvious example. As with the "Misuse Question" system designers must not live in "the best of all possible worlds" but understand the usual operational situations in which their technology will be deployed, and consider ways to avoid abuse or provide accountability for abuse within the system, or at least raise the profile of possible abuses, in system documentation.

The Re-purposing Question When developing a security system for aircraft, a particular set of legal and ethical questions are involved. A particular expectation (or lack of expectation) of privacy holds sway in an aeroplane. Many of the operational elements of a security system for aeroplanes will be equally applicable to other public transport situations such as trains, buses and ferries. However, the particular legal and ethical contexts can be significantly different. When considering a transfer of technology from one application area to even a highly similar one, therefore, a significant consideration of the validity of the ethical oversight, including PIA, needs to be undertaken.

People are Part of the System Although in terms of usability and achievement of operational objectives, the position of people in security systems is being taken more seriously (though probably still not seriously enough[MS02, MS05]). Designer of security systems must therefore consider how the inadvertent or untrained operator might use their system and thus invade the privacy of the surveilled.

In dealing with all of these question (and this is not an exhaustive list) the whole system needs to be taken into account. This "whole system" includes the broader social norms of the society in which the technology is to be deployed (consider the use of sniffer dogs in Iraq) as well as the operators of the technology. Ethical considerations, including respect for privacy, need to become a natural and important part of the design process. It has taken twenty years for this to even be approached for usability. The pace of change in security technology does not allow us the luxury of taking another twenty years to embed privacy and other ethical considerations.

Deployment decisions, operator training, restricted sale and distribution, legal regulation of use of systems, and transparency of justifications need to become watchwords for the designers, manufacturers, distributors, regulators and users of security systems.

References

[Com06] Chief Surveillance Commissioner. Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2005–2006. Published by the Stationery Office of the UK Government, 2006.
www.surveillancecommissioners.gov.uk/docs1/annualreport200506.pdf.

[Com07] UK Information Commissioner. Privacy impact assessment handbook.
www.ico.gov.uk/upload/documents/pia handbook html/html/foreword.html, Dec 2007.

[MS02] K. D. Mitnick and W. L. Simon. The Art of Deception. Wiley, 2002.

[MS05] K. D. Mitnick and W. L. Simon. The Art of Intrusion. Wiley, 2005.

[NA99] C. Norris and G Armstrong. The Maximum Surveillance Society: The Rise of CCTV. Berg, Oxford, 1999.

Organizational Motives for Adopting Privacy Enhancing Technologies (PETs) [1]

Uncertainty motivates individuals to seek information, as it is an uncomfortable state.
E. M. Rogers, Diffusion of Innovations, New York 2003

John Borking[2]
Borking Consultancy, Wassenaar, The Netherlands
jborking@xs4all.nl

1. Introduction

Cas and Hafskjold wrote: "So far PETs have not contributed as much as would be possible to the protection of privacy; partly because of a lack of availability of PETs, partly because of a lack of user friendliness" [32]. Leisner & Cas further pointed out that "PETs are insufficiently supported by current regulations; in particular it is not compulsory to provide the option of anonymous access to services or infrastructures" [33]. Sommer observed after four years of PRIME[3] research: "We still face major obstacles towards a deployment of such (PETs) technology in the field at a large scale (…) the part of convincing business to design their business processes in a way such that data minimization can be implemented as envisioned in PRIME will even be harder than has been the technological part" [34]. Is it a matter of resistance to change?

PETs have been defined as a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system [31].

However it seems that it isn't the user friendliness, the lack of availability of PETs or a resistance to change, but there are other reasons why PETs isn't used by governmental or commercial organizations.

A group researchers (Borking, Bos, Dijkman, Fairchild, Hosein, Ribbers, Tseng) have focused in the PRIME project [29] in 2007 and 2008 [35] on what business drivers lead organizations to adopt privacy enhancing technologies (PETs) for providing assurance for privacy. Although the concept of PETs has been introduced in 1995 [30], PETs have still been seen as a technological innovation. Putting into use of such an innovation can be regarded as a process of adoption [36]. The central question can be formulated as follows:

---

[1] This paper is partly based on the PRIME research reports F 1 till F4.
[2] Drs John J. Borking is a former data protection commissioner of The Netherlands and is since 2002 owner/director of Borking Consultancy in Wassenaar, The Netherlands
[3] EU research project PRIME (Privacy and Identity Management in Europe) project Contract No. 507591(2004-2008)

What factors impact the adoption of privacy-enhancing technologies tools in information systems as a measure to protect privacy sensitive data, and how do these factors affect the adoption decision?

Interviews in 2007 and 2008 [39] with representatives of the Telecommunications industry in Sweden and Finland; the Software industry, Government, Law firms, Health care organizations in UK; Consumer Electronics, Petro-Chemical industry, Gaming and Lottery organizations, Government and Property Insurance in The Netherlands; and the Telecommunications and Banking sector in Switzerland showed that the capability of an organization to innovate or to apply an innovation is important in today's competitive environment. If an organization lacks this capability it will fail in applying the necessary transformations and introducing innovation. This may result for these organizations in creating a competitive disadvantage [22].

As will be pointed out hereunder, for the implementation of PETs, certain maturity of the organization is required. It is highly unlikely those immature organizations will implement PETs, let alone that these organizations have any awareness of privacy protection. The level of maturity for Identity and Maturity Management (IAM) seems to be a strong indication for the introduction of PETs in an organization. There are strong indications that the Nolon Norton S curves for IAM, privacy protection and PETs are an indication of the time frame when companies are capable to implement PETs.

2. Technological innovations

An innovation is generally defined as the application of something new. According to Rogers [16] the question whether something new is an innovation has to be considered from a relative point of view. Something that in a particular environment or by a particular person is subjectively perceived as new can be regarded as an innovation. An innovation can also be related to many things, like an idea, a method, a technology or a product. Each of these types of innovations has its characteristics, which play a role in the adoption process.

Given the innovative character of ICT, research of innovation in particular technical innovations, tends to focus on technological innovations like software or electronic services [23]. The OECD [18] defines technological innovations as:

> *"A technological new product or process that includes a significant improvement and has been actually put into use. The technological new product or process consists of a variety of scientific, technical, organizational, financial and commercial aspects."*

Privacy Enhancing Technologies, given the relative recent introduction of the concept [2], the progress that is being realized with its application, and the new approach they offer with regard to privacy protection can be regarded as innovation.

3. Diffusion and adoption of technological innovations

A central theme in the research on innovation is in particular the way technological innovations are spread in a specific environment and how subsequently these innovations are being accepted and utilized. This area is known as ‘diffusion and adoption’ [6]. Diffusion relates to how innovations are spread across a specific society or industry [7]. Adoption is defined as the process through which a person or organization evolves from first getting acquainted with the innovation till its eventual utilization [37].

In the study of diffusion and adoption many studies try to identify relevant impacting factors, so that predictive statements can be made [11]. Three directions of research can be distinguished. Let’s first examine the factors that determine the speed, pattern and extent of adoption of a specific innovation. Second, the factors that make an organization suitable for adoption of a specific innovation can be a subject of research. Third, the former can applied to a specific innovation to examine what factors determine the adoption of that innovation by a specific innovation.

Rogers [16] considers adoption and diffusion as a process with a relatively known and constant pattern of evolution. He describes the rate of adoption as an S-shaped curve.

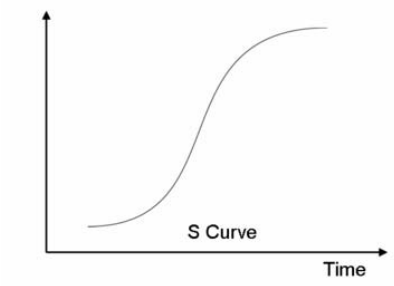


Figure 1 Rate of Adoption [18]: Relation adopters (Y) versus time (X)

Although the idea of the S-shaped curve (limited interest for the innovation in the beginning, followed by an increased interest leading to an intensified use, which eventually will level off) applies to all types of adoption, the slope may differ per innovation [18]. Others, who state that also partial adoption, as a middle road between adoption and non-adoption, is a viable possibility, have supplemented Rogers’ ideas; this reduces the contrast between adoption and non-adoption [1].

4. The role of Individuals and organizations in the process of adoption

Since the industrial revolution the process of adoption and diffusion of innovations generally followed what has been termed the "traditional model," a "top-down" process in which a management "mandate" introduced the technology and management perceptions, decisions and strategies drove adoption and diffusion. Successful adoption was highly dependent on the degree, stability and wisdom of management.

None of these technologies, however, has been generally available for individual or private use due to cost, scope or application. This deterred a "grass roots" technology adoption cycle, as it was nearly impossible to generate movement from the bottom up by influencing peers with demonstrations of successful applications. [37]

In the study of adoption two levels of adoption can be distinguished: the adoption by individuals versus by organizations [7]. In case of adoption by an individual the focus is on the decision making process that leads to the utilization of the innovation by an individual person. The individual is supposed to be able to exert authority whether or not to use the innovation. To understand this adoption, behavior models have been developed like the Technological Acceptance Model (TAM) and the Theory of Reasoned Action (TRA) [26].

The second level is the organizational level, where it is an organizational authority that decides to introduce an innovation. There are obviously relations between these two levels but also differences. Often it is first an organization that takes a formal decision to use a specific innovation, before the innovation is introduced. Next, however it often depends on the individual user whether the innovation is actually being used. Also the process of adoption by organizations is proposed to be more structured than the process of individual adoption [18]. Organizations tend to act more rational and posses better information than individuals.

Rogers [18] distinguishes five stages in the organizational process of innovation adoption: agenda-setting, restructuring, clarifying and routinizing. When the routinizing stage starts the innovation actually stops to be an innovation. The first two steps belong to the initiation phase, which precedes the formal decision and ultimately leads to a decision to adopt (or non-adopt). The last three steps belong to the implementation phase, which encompass all activities that lead to the eventual putting into use of the innovation (see Figure 2).

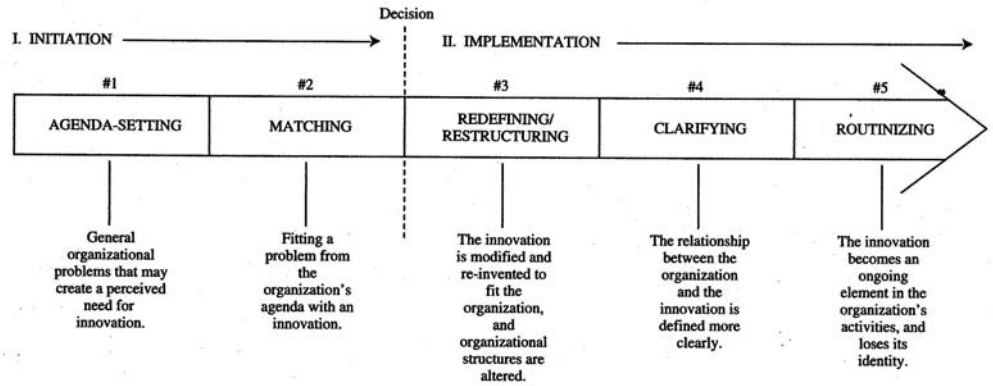


Figure 2 Stages in Innovation Adoption [18]

Zaltman developed similar descriptions of the adoption process [27]. Although there is no dominant theory on organizational adoption of innovation, Rogers' theory is considered to be very authoritative [8, 15].

Carr [37] pointed out that although Rogers [18], has been considered by many the "guru" of adoption/diffusion research since publishing *Diffusion of Innovations* (now in its fifth edition) in 1960, there are three important ways in which the adoption of interactive communications differs from that of previous innovations. 1) A critical mass of adopters is needed to convince the "mainstream" users of the technology's efficacy. 2) Regular and frequent use is necessary to ensure success of the diffusion effort. 3) Internet technology is a tool that can be applied in different ways and for different purposes and is part of a dynamic process that may involve change, modification and reinvention by individual adopters. Fairchild and Ribbers confirmed that IT based adoption are requiring a different approach and that there are specific effects of innovations in network organizations on inter-organizational relationships [35].

Internet technology actually embodies a number of technologies, like e-mail, databases, chat rooms, information and education resources, among others. Additionally, the Internet exhibits many elements that constitute a culture or community--language, symbols, rituals, interaction, and other elements of communication. It thus essentially becomes an environment into which users enter. "Visionary" innovation and "pragmatic" application can begin with grass-roots enthusiasts who enter this environment. [37]. Viewed as a culture or community, however, the Internet can be perceived as a threatening competitor to the established norms of an existing culture or community, such as an academic department or some other institutional entity, for example the use of e-mediation encounters resistance from the legal environment where most dispute resolution is traditionally still like in the 19th century [38].

5.Impacting factors of organizational adoption of technological innovations

Rogers distinguishes various variables that influence the process of adoption of innovations. First he describes characteristics of the innovation itself: relative advantage or benefit, compatibility, complexity, testability, and visibility of the innovation. He also points their impact is determined by the perception of these factors by the potential adopter, and not so much by how they are in reality. Next he distinguishes various variables that characterize the organizations, which are open to adopt innovation. These variables are based on the work of Zaltman [27]: the general attitude of top management with regard to change, centralization, complexity, formalization, internal relatedness, organizational slack, size and openness of the organization to the environment [35].

Rogers' Diffusion of Innovation [DOI] Theory has gained quite a broad acceptance; the variables have been tested in multiple studies and found relevant. Also Jeyarai et al. [12] and Fichman [8] found that three clusters of factors explain the organizational adoption behavior: factors related to the technological innovation, to the adopting organization, and to the environment of both former factors. They investigated over a hundred variables that have been researched in different studies. They also performed an empirical test on the best predicting factors for the organizational adoption of IT-based innovations. Combined in clusters the dominant factors appear top be those related to innovation characteristics, organizational characteristics, and environmental characteristics [36]. Tung & Reck [23] reach this conclusion in their study.

Others have emphasized other influences on the adoption process: Fichman [8]: argues that adoption of IT based innovations require a different approach. Fichman [8], Riverea & Rogers [17] and Greenhalgh [10] point to specific effects of innovations in network organizations on inter-organizational relationships. The approaches of Jeyarai, Fichman and Rogers form the foundation for the Conceptual Model shown in Figure 3.

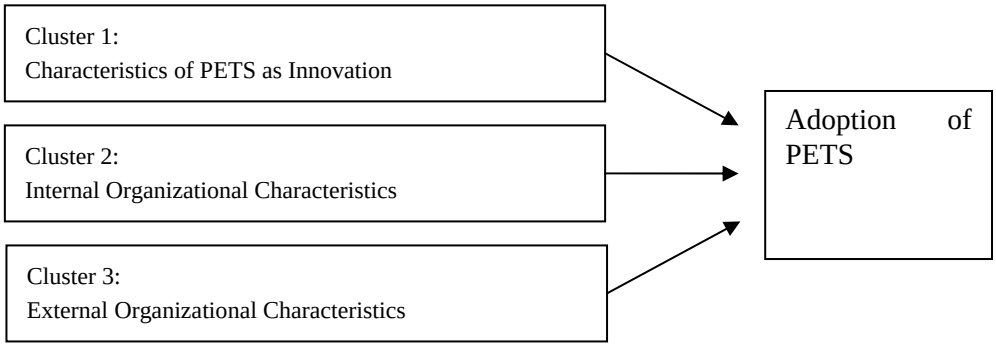


Figure 3. Conceptual adoption Model [35,36]

The first cluster of factors encompasses those variables that are related to the technical innovation itself, and so to PETs. The second cluster looks at those variables that are related to the internal characteristics of the adopting organization. The third cluster contains factors related to the environment of the adopting organization and innovation. In case of PETs, in particular privacy policies and regulations, and level of enforcement seem to be particularly relevant.

We will look in more detail at the variables introduced by Rogers [18] and Fichman [7, 8].

Rogers [18] distinguishes five innovation characteristics and eight organizational characteristics, which affect the organizational adoption of innovations.

Innovation characteristics

Relative advantage or benefit (+): the advantage offered by the innovation, compared to the former practice or technology

Compatibility (+): The extent that an innovation resembles its predecessor

Complexity (-): The effort needed to learn how to use the innovation

Testability (+): The extent that small-scale experiments with the innovation are possible

Visibility (+): the extent to which the innovation is visible for the outside world

Organizational Characteristics

Top Management's attitude with regard to change: How open is top management to accept the changes that accompany the innovation?

Centralization: The degree of concentration of power and management

Internal Organization complexity: The extent that members of an organization possess specialized knowledge and expertise.

Formalization: The level of bureaucracy in an organization

Internal relatedness: The extent that internal members of the organization are interrelated

Organizational slack: The extent that an organization possesses uncommitted resources.

Size: The size of the organization

Openness: The degree that organizations are in contact with other organizations

Fichman [8] compared different adoption studies and built an encompassing model that explains organizational adoption of complex information technology innovations. The model consists of three clusters, while each cluster contains a few groups of factors.

The three clusters are:

- The Technology & Organization Combination: factors that describe the relationship between the innovation and a specific organization. This boils down to the fit between the innovation and the organization, the perception of organizational characteristics and factors that describe the possibilities for an organization to implement the innovation.

- The Technologies & Diffusion environments: those factors that describe the innovation and the specific environment from which they emanate. These are in particular the innovation characteristics and possible roles of advising institutions.

- The Organizations & Adoption environments: factors that describe the adopting organization and their environment. These are organizational characteristics and characteristics of the environment and industry.

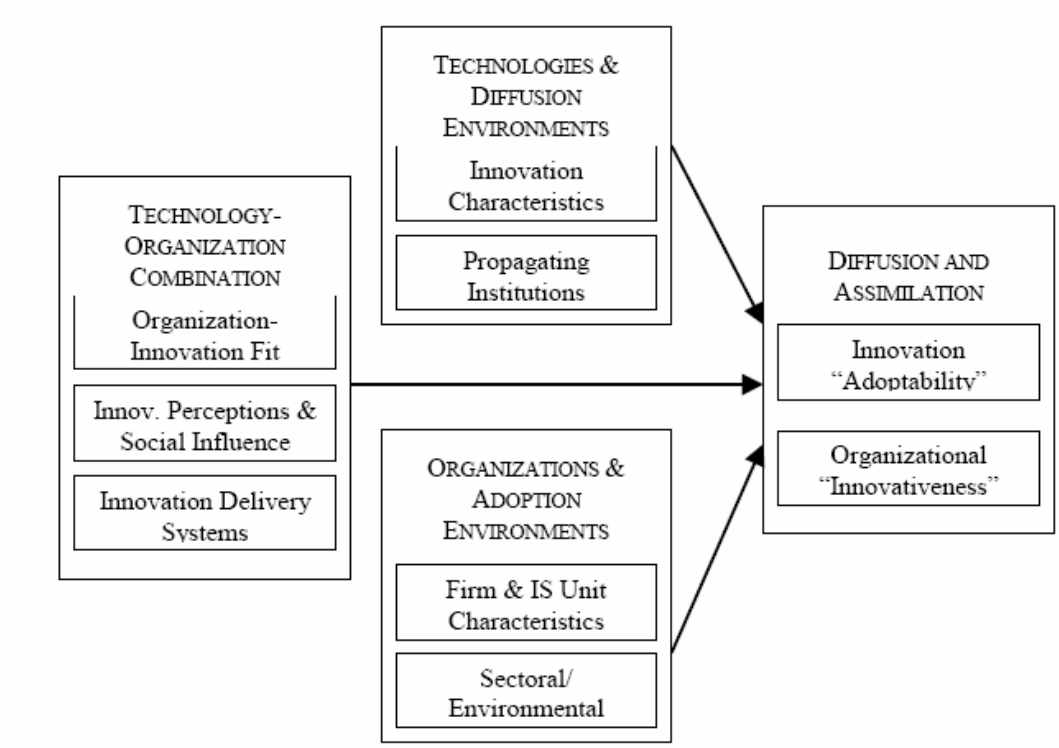


Figure 4. The encompassing Model [8]

6. Interviews with Experts

In order to find variables that characterize each cluster, the literature analysis has been combined with expert interviews. Factors that have been proposed to be relevant in the literature have been compared with the results of expert interviews, and vice versa. Thirty experts in the field of PETs have been interviewed [35,36,40]. The results of the interviews are presented in table 1 below. The variables mentioned by the experts and organizations have been grouped according to the categories innovation, internal organization and environment.

Table 1 Results of Interviews of Experts by Category

Factor: Innovation	***Results***
Relative benefit	Positive
Complexity	Negative
Costs	Negative[4]
Role of advisory institutions	Positive
Social recognition / visibility	Positive
Pets woven into business processes	Negative
Factor: Internal Organization	
Complexity of organizational processes	Negative
Presence of key persons	Positive
Ties with advisory institutions	Positive
Perception of privacy 'standards'	Negative
Type of the data processed (risk related)	Positive
Factor: Environment	
External pressure by privacy laws	Positive
Complexity of privacy laws	Negative

Relative benefit

The advantage of PETs is that it offers a clear privacy protection, which, when properly applied, is in line with legal requirements. The potential relative benefit compared to other protective measures is big. It however appears to be difficult to value in economic terms the relative benefits of PETs compared to other protective measures. This is caused by the existing ambiguity around PETs and privacy. As a result, often more conventional measures are chosen instead. ROI equations are under development for quantifying the benefits of the PET investment [35, 41].

Complexity

PETs are perceived as a complex innovation. The implementation of PETs requires specific expertise in different disciplines. Except IT expertise also legal expertise is needed; this combination of is very scarce and has to be acquired externally.

[4] When calculating the Return On Investment on PET investments an attitude change towards adoption is noticeable [41]

Costs

PETs are perceived as an expensive innovation. Much depends however on the moment those PETs are introduced. If the introduction is when a new system is put into use, then costs are generally at an acceptable level. This is also basically the only realistic option. PETs are simply too complex to apply to existing systems, costs are then being perceived as higher than those of traditional measures. However ROI equations for PET investment may assist in justifying the investment costs [35, 41]

Role of advisory institutions

Some organizations can play a key role in the diffusion of innovations. The Dutch Data Protection Authority has assumed this role with regard to PETs in the past, especially with regard to large projects. This role and the attention given to PETs have impacted its adoption. At the moment the DPA does not promote the use of PETs actively anymore, with a considerably lower rate of adoption as a result.

Social Recognition / Visibility

The use of PETs does not receive a lot social recognition, which is the result of its limited visibility. Also privacy protection is not an issue with which organizations try to differentiate themselves. However when the PETs application is visible for the public for example by advertising: *PETs inside*, then it is a positive adoption factor

PETs woven into business processes

An important characteristic of PETs is that its implementation requires integration in information systems. This requires legal and technical (ICT) expertise.

Complexity of organizational processes

PETs-measures usually have to be customized for a specific organization or process. The more complex this is, the more difficult it is to implement PETs.

Presence of Key Persons

The utilization of PETs often depends on specific key persons in an organization, who know the concept and take the lead in the adoption process. Such a person has a strong impact on the adoption of PETs.

Ties with advisory institutions

The use of PETs sometimes depends on the ties that an organization has with advisory institutions (e.g. DPA). An organization that has no links with such institutions is not likely to put PETs into use.

Perception of privacy standards.

Privacy standards are often not perceived as being very important; also the consequences of not complying with the law aren't considered as important. As a result the adoption of PETs is not high on the management agenda.

Type of processed data

When the level of risk associated with privacy breaches is high, then, based on the law, there is a bigger incentive to apply PETs.

Pressure by privacy laws

Privacy laws exert little pressure on organizations to really put PETs into use. Only in a few cases the law refers to PETs, however the decision makers are left free what to choose as protective measures.

The EU privacy directives are of a too general ad abstract character. In general there is little awareness of PETs. The focus of decision makers is on the key business processes; privacy is often a secondary issue. However the interest for security is increasing. There is also very limited demand for privacy audits, because there is no felt need to have one.

Complexity of privacy laws

Organizations often do not know/understand what privacy laws require them to do. Because privacy laws are overly complex and ambiguous, they do not use the right set of protective measures.

7. Conceptual Model for the adoption of PETs

In practice, it does not matter so much how complex an innovation really is, however what matters more is how a subject perceives its complexity. Although compared to adoption by individuals, adoption by organizations shows more rationality, perception plays an important role also on the organizational level. Fichman [8] mentions social appreciation that goes together with the utilization of the technological innovation.

The conceptual model is shown in Figure 3 above. This model encompasses the variables that have been identified in two of the three case studies done in the Masters thesis [36]. We then discuss by cluster the effect of the different variables in Table 2, and the support of the adoption factors using one case study as an example.

Table 2: Clusters and variables per cluster [35]

Cluster 1	
Characteristics of PETS as Innovation	***Effect***
Compatibility	Negative
Complexity	Negative
Costs	Negative
PETs woven into business processes	Negative
Cluster 2	
Internal Organizational Characteristics	***Effect***
Structure and size of the organization	Negative
Perception and level of awareness of privacy regulation	**Positive**
Diversity in Information Systems	Negative
Individual Ties with advisory institutes	**Positive**
Cluster 3	
External organizational Characteristics	***Effect***
Pressure by privacy legislation	**Positive**
Differences between public and private organizations	Negative
Existing offer of PETs measures.	**Positive**

In Table 2, only those factors have been incorporated that were supported by two of the three case studies. Factors that were found to be relevant in only one case study are listed in the table below.

Table 3 Adoption factors supported by a minority of case studies

Overall Factor	***Effect***
Visibility and Social appreciation	**Positive**
Role of advisory bodies	**Positive**
Support by management and key positions in the organization	**Positive**
Complexity of privacy regulation	Negative
Relations and position public/private organizations in the chain	Negative

The model shows that a number of factors are perceived to have a negative impact on the adoption process. One assumption is that PETs is difficult to implement efficiently and effectively. Also the internal organizational characteristics have a negative impact. Although there is enough code developed, the limited offer of PETs tools by software suppliers appears to have a negative impact. Only the legal and regulatory pressure with regard to privacy protection has an undivided positive impact on the adoption process. However, the existing legislation provides too little reference to the concept of PETs, to make a difference in the

adoption process. The promotion by advisory bodies appears to have a strong positive influence [35].

A conclusion of this study is that the adoption of PETs is problematic. There is only a limited use. Looking at the final model, in particular those factors that are related to regulatory and legal compliance, to improved coordination and advice and information with regard to PETs, seem to help to solve this problem. The relative advantage of PETs is perceived to be zero. However in interviews with large international organizations the use of PETs in relation to preventing reputation damage is seen as positive, especially when a positive ROI could be demonstrated. Both informational activities and adaptation of the law seem to be necessary. Legal requirements are generally observed; however in privacy laws there is insufficient reference to PETs. Also the minimum level of privacy protection required by the law is perceived as insufficient as an incentive to apply PETs [35].

9. Towards A Process Maturity Model for Privacy and PETs

To examine under what conditions an organization would adopt PETs into its business processes, the researchers explored how an IAM maturity model can be adapted to examine privacy adoption maturity in organizations. The hypothesis behind the choice for the IAM maturity model is that as protection of personal data is closely linked with identity issues, the increased attention for identity in the organizational processes must lead to the awareness of informational privacy.

A maturity model is defined as *"a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organization develops and adopts new processes and practices, from which it learns, optimizes and moves on to the next level, until the desired level is reached."* [19]

During the last decade several maturity models have been developed in specific research areas such as business IT alignment, software development and information security. All of these models have one thing in common; they all describe the maturity of one or more processes within an organization. As a basis for this IAM maturity model, a number of existing models were examined. In summary, the researchers examined the maturity models of Nolan Norton, *CCMi* from the Software Engineering Institute (SEI), and Dutch INK maturity models, and all had some influence on this IAM model [35].

The descriptions of these maturity levels differ among the models, but are quite similar in general. Every model characterizes the first maturity phase as being chaotic and dealing with processes on an ad hoc basis. The second maturity level is characterized by the planning of processes. The third maturity level is characterized by the implementation of standards aimed at particular processes and outputs for processes are defined. Quantitative management characterizes the fourth maturity level.

Processes and quality are controlled based on quantitative measures. Based on the measures taken out of the quantitative measures implemented in maturity level four, maturity level five improves the organization. These improvements are continuous, incremental and connected to the business objective measures [5, 9, 19, 25].

The following general phase descriptions can be discerned:

Phase 1: Only few processes have been defined and processes are conducted on an ad hoc base.

Phase 2: Processes that seem to work and be in order are repeated.

Phase 3: Processes are standardized and documented to review if they are executed accordingly.

Phase 4: Performance and success are measured and quality measures are done

Phase 5: Processes are systematically improved with the help of quantitative feedback of results, test results and innovative ideas.

Based on a KPMG [13] model, researchers then integrated maturity phases into these processes, and developed an IAM maturity model shown below:

Authentication Managment	No authentication means	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Authentication Requirements based on a one time survey	Authentication Requirements based on continuous risk analysis	Authentication requirements based on continuous risk analysis and are continuously adjusted
User Managment	Double and inconsistent entries because of chaotic and ad hoc processes	Entries can be double but they are consistent	Central registration, Limited user group, manual procedures	Central registration, controlled authorization processes, manual procedures	Central real-time controlled authorizatino sources, automated procedures
Authorisation Managment	No authorization matrixes, authorization is defined ad hoc	Authorization matrixes defined but are not updated	Authorization matrixes are updated periodically	Role Based Access Control used for critical applications	Role Based Access Control for all applications and continuous updated authorizations
Provisioning	Manual process locally	Limited Automated unreliable processes locally	Limited Automated but reliable processes locally	Limited Automated and reliable for multiple sources	Automated and reliable for multiple sources
Monitoring(Audit)	No responsibilty delegated into a AO/IC organization	Sporadically delegated responsibility of AO/IC	Partial delegation of responsibility to AO/IC	Full responsibilty to AO/IC	Full responsibility to AO/IC with periodic reporting
	Immature	**Starting-up**	**Active**	**Pro-Active**	**Top Class**

Figure 5 Conceptual Identity and access management maturity model

10. Identity and Access Management (IAM) Maturity Model

The maturity model in figure 5 can in turn be translated into a more general description of maturity phases for IAM in general. This means that the whole IAM situation is described per

maturity phase. Describing the situation in general leads to a more practical and understandable image of the Identity and access management processes.

Maturity Phase Descriptions across IAM processes:

- Maturity phase 1: “Immature”: In this phase the notion of Identity and access management begins to dawn within the organization. No or very little applications or processes are in place to facilitate IAM. Monitoring and audit are virtually nonexistent and provisioning is done manually. Means of authentication are very rudimentary such as local username and/or passwords. User profiles are maintained locally and can be doubled and inconsistent. Authorizations are not regulated and authorizations are assigned on request and are not based on an authorization matrix. This leads to a situation in which user profiles exist locally in the company’s database and another user profile most likely exists on their company computer. This profile provides access to the complete array of programs installed on that one pc. Provisioning is done manually at each workstation; this most likely cannot be done centrally yet. User profiles are only updated locally by the administrative personnel and the profiles on the workstations are either maintained by the employee themselves or not at all.

- Maturity phase 2: “Starting up”: In the second stage of maturity the company is starting to realize that IAM is needed. Authorization matrixes are developed and authentication requirements are arbitrarily formulated based on user requirements. E-identity databases are improved to the point, that they contain double but consistent entries. Provisioning activities are becoming automated but are still done locally. Monitoring and audit activities are getting started although in a highly sporadic fashion and responsibility is only sometimes delegated to AO/IC. Activities that are only now starting to be executed such as automated distributed provisioning and the creation of authorization matrixes and authentication requirements are not very reliable or periodically updated.

- Maturity phase 3: “Active”: Maturity phase three is in essence an improvement on phase two. Most of the processes are still the same, but are executed regularly or have become regulated. Authentication management has improved significantly since it is no longer based on ad hoc user requirements, but on a one-time survey. User management also has improved quite a bit; users are registered centrally and are positioned in a user group. Provisioning is still limited to a certain number of applications and executed locally, the automated provisioning however has become more reliable. The responsibility of the IAM processes is increasingly delegated to the Monitoring and Audit activities.

- Maturity phase 4: “Pro-Active”: In this phase the authentication requirements are updated periodically based on continuous risk analyses that are executed. User management still is manual process it however now is a total centralized process that controls all user registrations. Authorization management is characterized by the introduction of techniques such as role based access control (RBAC) for critical applications. This means that the access rights assigned to the user are based on the access rights given to the group. Provisioning remains automated and reliable but the scope of provisioning is enlarged from local to multiple provisioning sources. Responsibility for Monitoring and audit becomes the total responsibility of the AO/IC organization.

- Maturity phase 5: “Top Class”: The general improvement for this maturity level entails continuous improvement and/or adjustment of the IAM processes. The great change for user management is that authorization processes no longer have to be done manually, but now become automated. Authorization management is changed in the way that RBAC is now implemented for all application and authorization rules are adjusted real-time. Provisioning has become automated and reliable for all provisioning sources. Monitoring and Audit not only controls now but also acts on its control activities by regular reporting.

Through all of these five maturity phases the awareness and importance of IAM processes increases within the organization. The organization going through all these sequential phases not only needs to adjust its identity and access management processes, but also its own organizational structure and policies need to be adjusted. These adjustments like the adjustments to the IAM processes need to be evolutionary not revolutionary. Since IAM can entail the creation of roles or positions within the existing organizational structure, the impact of an IAM implementation can be quite significant. In order to deal with these changes the organization needs to be ready and willing to accept these changes or adjust the IAM project to suit the organizational structure, meaning that the organization and IAM need to be adjusted to each other for IAM to be successful after implementation. This could be an argument to introduce organizational structure as a part of the IAM maturity model. However there already exist organizational maturity models for organizations dealing with the questions of IT projects [4, 21]. Introducing organizational maturity into the maturity would also introduce organizational facets that are not immediately related to Identity and access management. Therefore that organization is only added as a “foundation” into the IAM maturity mode [13].

Top Class	Authentication requirements based on continuous risk analysis and are continuously adjusted	Central real-time controlled authorizatino sources, automated procedures	Role Based Access Control for all applications and continuous updated authorizations	Automated and reliable for multiple sources	Full responsibility to AO/IC with periodic reporting
Pro-Active	Authentication Requirements based on continuous risk analysis	Central registration, controlled authorization processes, manual procedures	Role Based Access Control used for critical applications	Limited Automated and reliable for multiple sources	Full responsibilty to AO/IC
Active	Authentication Requirements based on a one time survey	Central registration, Limited user group, manual procedures	Authorization matrixes are updated periodically	Limited Automated but reliable processes locally	Partial delegation of responsibility to AO/IC
Starting up	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Entries can be double but they are consistent	Authorization matrixes defined but are not updated	Limited Automated unreliable processes locally	Sporadically delegated responsibility of AO/IC
Immature	No authentication means	Double and inconsistent entries because of chaotic and ad hoc processes	No authorization matrixes, authorization is defined ad hoc	Manual process locally	No responsibilty delegated into a AO/IC organization
	Authentication Managment	**User Managment**	**Authorisation Managment**	**Provisioning**	**Monitoring(Audit)**
	Organization				

Figure 6 IAM maturity model with organization foundation

11. PET Stages Model combined with the Maturity Model

In the White book on Privacy Enhancing Technologies by Koorn et al. [14], all is stated that PETs is composed out of several technologies divided in four different PETs stages (shown in Figure 7). These technologies in turn require a certain IT infrastructure. It also becomes clear from the White book that implementing PETs requires a solid foundation in the form of Identity and access management. With the help of Identity and access management, PETs tries to minimize the use of and access of sensitive personal data. Especially the mentioning of the PETs Secured Access in Figure 7 makes this clear. Secured Access however is only the first step for PETs. Privacy Enhancing Technologies also strive to segregate sensitive information in order to secure a person's identity. Not only segregation however is used to achieve this goal. Depending on the organizational information needs, information can also be immediately removed after use or not even registered in the first place.

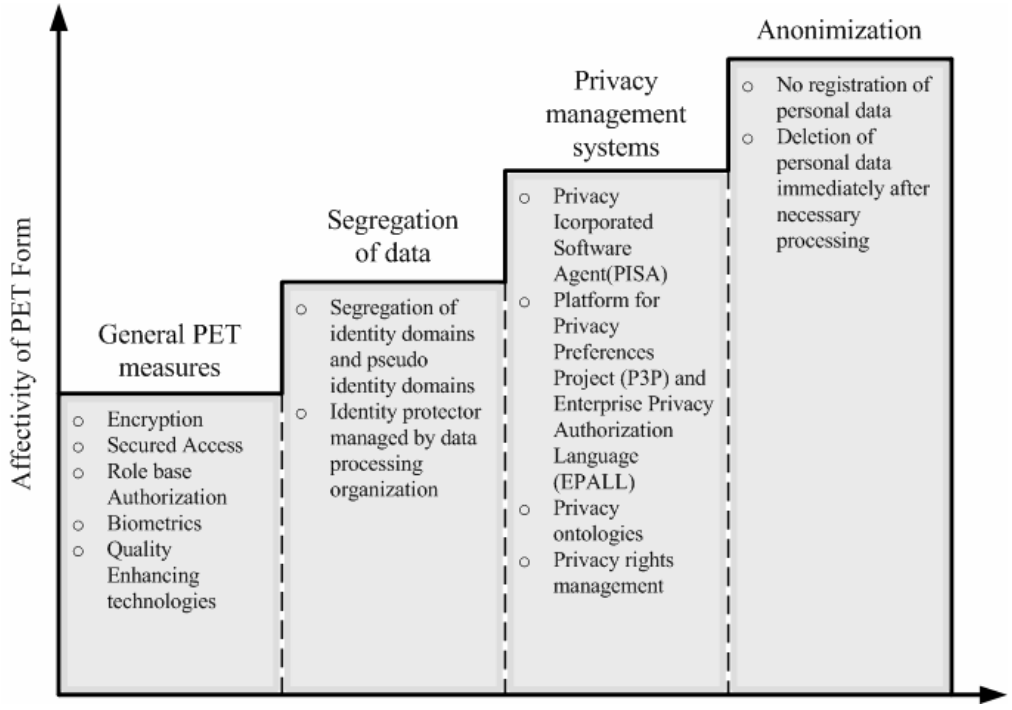


Figure 7. Staged Affectivity of PETS including used technologies per stage

If the rights to access can be bound to a certain group, profile, person or user within an organization then IAM can be used to make sure that the user or user group only gets access to the information for which they are authorized. IAM then can also be used to provide the means of identification to make sure that the right user gets access to the user profile that is authorized to access certain sensitive information. Next to user management, authentication management and authorization management, provisioning and monitoring and audit can also play an important part in a PETs implementation. For instance when a central database of information is accessed by different organizations provisioning (automated or not) can play an important to keep user accounts for that database up to date at the different locations. Monitoring and Audit plays an important role when reviewing the current status of user

accounts and controlling if authorized users only are accessing data. Thus depending on the requirements of the organization on its PETs implementation a certain level of maturity is required for the relevant IAM processes.

For the implementation of PETs, certain maturity of the organization is required. It is highly unlikely those immature organizations will implement PETs, let alone that these organizations have any awareness of privacy protection. The level of maturity for IAM is a strong indication for the introduction of PETs in an organization [35].

For IAM, it can be assumed that if the rights to access can be bound to a certain group, profile, person or user within an organization then IAM can be used to make sure that the user or user group only gets access to the information for which they are authorized. IAM then can also be used to provide the means of identification to make sure that the right user gets access to the user profile that is authorized to access certain sensitive information. Next to user management, authentication management and authorization management, provisioning and monitoring and audit can also play an important part in a PETs implementation. For instance when a central database of information is accessed by different organizations provisioning (automated or not) can play an important to keep user accounts for that database up to date at the different locations. Monitoring and Audit plays an important role when reviewing the current status of user accounts and controlling if data is accessed by authorized users only. Thus depending on the requirements of the organization on its PETs implementation a certain level of maturity is needed for the relevant IAM processes. By combining the PETS steps and the maturity model the maturity model can predict when PETs will be used in which stage of development of the organization.

Based on this model it is predicted that PETs will be applied by organizations in the Top Class and Pro-Active maturity level, with the exception for organizations that update authorization matrixes periodically (organization at the level: active). See figure 8. There are exemptions for those organization that belong to the category of (micro/mini) SMEs where trust is a critical success factor, like in the medical profession, barristers, notaries etc. Although the processes mentioned in the maturity model are non-existent, it may be expected that those SMEs will protect personal information of their clients encrypted or will use rudimentary PETs tools.

Authentication Managment	No authentication means	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Authentication Requirements based on a one time survey	Authentication Requirements based on continuous risk analysis	Authentication requirements based on continuous risk analysis and are continuously adjusted
User Managment	Double and inconsistent entries because of chaotic and ad hoc processes	Entries can be double but they are consistent	Central registration, Limited user group, manual procedures	Central registration, controlled authorization processes, manual procedures	Central real-time controlled authorizatino sources, automated procedures
Authorisation Managment	No authorization matrixes, authorization is defined ad hoc	Authorization matrixes defined but are not updated	Authorization matrixes are updated periodically	Role Based Access Control used for critical applications	Role Based Access Control for all applications and continuous updated authorizations
Provisioning	Manual process locally	Limited Automated unreliable processes locally	Limited Automated but reliable processes locally	Limited Automated and reliable for multiple sources	Automated and reliable for multiple sources
Monitoring(Audit)	No responsibilty delegated into a AO/IC organization	Sporadically delegated responsibility of AO/IC	Partial delegation of responsibility to AO/IC	Full responsibilty to AO/IC	Full responsibility to AO/IC with periodic reporting
	Immature	**Starting-up**	**Active**	**Pro-Active**	**Top Class**

Figure 8 Potential areas for PET application (red areas)

12. Is there a Business Case for Privacy?

In order to best understand the likely adoption of PETs we must first understand the challenges that privacy poses for organizations [35]. This can be done best through engaging with experts and practitioners. To achieve this, the researchers conducted a number of consultations with industry experts, through direct discussions and by using a workshop-format.

Traditionally when researchers ask the question whether organizations have some inherent interest in privacy, a list of drivers emerges. These drivers include: compliance with legal obligation, fear of reputation damage from privacy failure, the need to generate trust with clientele, and the promotion of a good corporate practice. Yet if this was truly the case then privacy enhancing technologies would be already implemented everywhere across both industry and government organizations. Reality appears more complex.

There is much doubt amongst experts that there is in fact a well-structured business case for privacy. The traditional drivers are insufficient, in particular:

- Compliance is not taken particularly seriously, since there are so few investigations and even fewer penalties [35].

- Recent penalties, however, such as the ruling against Nationwide Bank in the United Kingdom who was fined nearly £1 million by the financial regulator for inadequate response to a data breach, are considered an opportunity for revisiting this concern [40].

- Reputation and Brand Damage is not an assured result of public disclosures of privacy failures. That is, research and experience show conflicting results on whether

organizations actually experience damages to their reputations from data breaches. Amongst experts there is a high level of skepticism that data breach reporting actually hurts companies through a loss of customers, though there has been some research indicating that stock market fluctuations do take place after the announcement of a breach [40].

- However, a several interviews of researchers in 2008 in the telecommunication, banking and property insurance market showed a strong positive correlation between privacy incidents and reputation damage that resulted in court cases, considerable damages and loss of customers. It seems that we lack enough empirical data as privacy incidents aren't reported to the data protection authorities [39].

- The notion of 'generating and maintaining consumer trust' is a large and perhaps unwieldy goal that is never quite verifiable. While this terminology permeated much of the discussion around e-commerce in the 1990s increasingly there is less being said today about trust. Privacy has not yet emerged as a differentiator in the marketplace — if trust were so important then certainly some organizations would be advertising their privacy-friendly practices quite vigorously [40].

- There is much faith in the idea that protecting privacy is merely another way of showing good corporate practice, but it is only recently that discussions have emerged about including privacy within corporate social responsibility regimes [39].

Organizations do not currently understand the nature of the risks posed by the processing of personal information. Just as it took organizations quite some time to learn about information security, some believe that this is how we can account for the lack of understanding about privacy. But as storage costs spiral downwards organizations are collecting and retaining as much information as possible — though it is possible that data breaches and other security concerns are finally causing some re-consideration of this trend. This would all change if a privacy impact analysis with examination by the Data Protection authorities would be legally mandatory.

Another analogy that emerged from discussions is that privacy may follow the same course as 'Total Quality Management' in that privacy can be seen as a means of 'tightening up the ship', in that it will help in better information management. This approach highlights that privacy may not be the 'good' that is being delivered (or sold) but instead the rise in consumer and organizational confidence/trust is the ultimate goal [40].

Privacy also falls into that odd area between 'social responsibility' and 'compliance'. While oil companies gain credit for giving money for research into alternative fuels, this is not perceived as a regulatory-burden (at least not yet). Privacy suffers because it is seen as a compliance issue and insufficiently as a good social practice. But in discussions with experts on this matter, they felt that there was much room for growth in this domain, particularly if privacy management is eventually seen as part of an organization's general attitude. That is, if a firm is seen as negligent in the processing of personal information, consumers and other firms should begin questioning whether this negligence spreads to other business domains within that firm such as staffing policies, or even the honoring of warranties. This requires however transparency of the market. A privacy seal as developed now in the EU research project EuroPrise [42] might be a stimulus.

To rectify this lack of appearance of a social goal, which is considered essential for a widespread adoption of privacy practices, we could move the emphasis of privacy invasions upon three 'harms': the harm that is created for the individual and the consumer; the harm to the corporation due to the time and expenses in rectifying the root problem and its effects; and the harm to society as a whole due to the reduced confidence in the sector and perhaps across sectors. Once privacy failures are emphasized on all these levels then a positive demand for privacy within organizations may emerge with every privacy disaster, leading to the ultimate goal of seeing privacy as a differentiator in the marketplace.

Throughout the discussion amongst workshop participants and with experts in the field, a consensus never emerged on whether there was a specific business case for privacy. The discussants appeared unsure of whether there was truly a business case for privacy or if we all wished it were true. Therefore the best way to summarize answer to this question is that:

1. Indeed, there may be a business case for privacy and this could be shown particularly after a privacy failure where a positive demand for privacy emerges and this leads to privacy becoming a differentiator in the marketplace.

2. There may not be a business case for privacy per se but there is a business case for better management of information resources within organizations in order to create confidence within the organization, across the supply chain, and with consumers. This better information management is perhaps best done through privacy management.

13. Validating the Conceptual Model

The interesting challenge in trying to 'validate' a conceptual model is that it is not so easy as to present it and demand responses. That is, perhaps conceptual models aren't useful to put out for consultation. When the conceptual model was presented, few discussants found it particularly interesting as a guide forward. More important, however, is that the model, with some modifications in detail, serves as the ideal analytical tool for sense making of all the feedback from the discussants.

Technological Characteristics

Surprisingly there was little discussion of the particular characteristics of the potential technological solutions. In fact there was some doubt that technological solutions are even reasonable: considering how little money is actually spent on privacy management within organizations, and the smaller amount that is expended on technological solutions, there was considerable doubt that technologies would be acceptable. This certainly validates the view that relative benefit and advantages of a technological solution is an issue, though the level of doubt is not promising [40].

The difficulty in integrating privacy solutions, whether technological or service-related, into organizational processes was highlighted. Repeatedly discussants drew links to privacy solutions and information management: if privacy techniques could not be sold as privacy techniques they could be better seen as a means of cleaning up the organization’s information management practices, e.g. database cleaning exercises. This linkage indicates that the characteristics of the technology matters: it must be able to not just limit data but also adequately manage data flows.

Data management techniques are not only required for within the organization but also for across organizations. That is, privacy is increasingly being seen as the management of information across the 'supply chain' or with third party organizations. A technological solution would have to cater for this broader goal.

Discussants seemed relatively uninterested in the role of advisory institutions in the decisions about technological characteristics. Regulators are considered important but not as part of the consideration of technologies. This may change as privacy breaches come to dominate business privacy concerns as regulators may choose to re-open dialogue about the role of encryption and other such technologies to minimize damages, but this was not seen as an immediate or pressing component.

Internal

Experts in the field had a general concern that organizations were not overly concerned about compliance with legal requirements. In fact, there was a feeling that organizations aren't overly concerned about privacy altogether. This seriously inhibits the adoption of privacy enhancing technology. The discussion with experts about possible ways forward gave results that are in strong harmony with the conceptual model.

There was a distinct sense that the nature of the organizational processes mattered greatly. There was also a general sentiment that organizations often manage information poorly. Correcting this situation was considered a necessity, through cleaning up the data stores, to then integrate the newer cleaner data with improved business processes in order to maintain the integrity of this data over the longer term. The type of data processed was also considered an essential component of this: financial data and medical data were most often mentioned as risky in the case of breaches [40].

Leadership and buy-in were repeatedly mentioned as well. Executive leadership and buy-in was mentioned repeatedly, though with the scepticism about the need for compliance it was doubtful that this could be realized. One popular idea was to make data protection law one of the number of laws that company directors have a legal duty to uphold. Doing so could positively enforce privacy throughout organizations.

Interestingly, marketing departments were considered essential. Marketing departments have the triple role of being quite rich and influential within organizations, responsible for much of the data collection and analysis, and potentially they could be interested in marketing the organization as privacy-friendly [40].

Yet the strongest factor in the consideration of privacy within organizations was internal culture [35]. Though the very notion of a culture of privacy protection within organizations was considered a recent phenomenon, it was repeatedly stressed that a culture of privacy, re-enforced with strong responses from management for breaches of policy, is perhaps the strongest driver of them all. While a strong culture could possibly be seen as an inhibitor of PETs adoption, it was also seen as a necessity for the success of PETs within an organization. For instance, if PETs was adopted to manage access controls, this could be simply circumvented through staff abusing their roles or privileges — and this is a problem that only a strong privacy culture could manage.

Advisory institutions were discussed, but in the UK rarely were regulators raised as key factors to the internal adoption of PETs. Discussants placed a greater emphasis on industry associations and standards, though their full effects were not fully contemplated [40].

External

There was a great deal of discussion about external factors. These can be divided into regulatory, legal, social and market factors. Experts felt that privacy law was poorly regulated. Fines were too few and far between, and even then they were minimal. Stronger regulators could play a larger role in privacy protection, and in turn they could promote privacy technologies. But the general consensus was that the current situation was unlikely to promote PETs adoption.

It is possible that privacy law itself is not strong enough. Examples were drawn with laws in some countries that place explicit barriers on the use and trade of information and how this led to stronger consideration of privacy within organizations. With lax laws and weak regulators there was little sense of the need to consider privacy. This is a slight difference of interpretation from the conceptual model where privacy law is seen as a positive promoter of PETS. This may be true but the law, along with the other factors, should be well formed and should be perceived as such in order for it to be a strong positive factor.

But law and regulation was not felt to be a positive promoter of PETs adoption. The general attitude was that compliance was not a good motivator for adoption of any form of technology, as was evidenced by the adoption of regulation-enforcing technologies in other domains, e.g. know your customer rules for banking, technologies for adherence to environmental regulations, etc.

Market and social factors were seen as the greater forces behind privacy and PETs adoption. Together these two factors could introduce changes in both consumer and organizational practices as consumers became more educated and demanded greater flexibility while organizations became more interested in promoting consumer confidence and with this advanced confidence, promoting new and enhanced services. Companies could then try to differentiate themselves from other competitors through the adoption of privacy practices.

For privacy to become a market differentiator, social factors would first have to take root. The social harm to privacy invasion would have to be better articulated. For instance, the lack of confidence in disclosing personal information has led to customers refusing to disclose personal information for fear of data breaches and identity theft. If identity theft increases and becomes an issue of widespread concern, it is possible that it would seriously damage trust between consumers and data collectors. Then organizations would find themselves scrambling to enhance confidence [40].

Privacy as a market differentiator could arise without widespread social changes; such as we have seen with the movements in the market surrounding corporate social responsibility. Here, organizations take leadership roles even though there may not be immediate financial compensation, because of the value of the organization’s reputation. An organization taking such an approach could use PETs as a means of further certifying their privacy-protective approach.

Cultural differences

During the interviews in different member states of the EU it became apparent that there are cultural differences. The interviews in the UK showed a lesser privacy consciousness than in Sweden, Switzerland and The Netherlands.

In Stockholm the representatives of the telecommunications industry stated that “Sweden is probably the most high–trust society in the world; this imposes a responsibility for XYZ to respect that trust and with that the privacy of the customers.” The relationship in Finland is mainly based on trust, the damage in a privacy incident is much higher, because it effects the core of trust”. Never the less the interviewed managers believed that “Unless privacy becomes an (business) opportunity, it will not be high on the management agenda. (...) Main vision is to offer so much privacy to meet customer demand being different in Kazakhstan (one of the countries were the organization operates) than in Sweden”.

In Zürich the interviewed bank managers interpreted privacy as a synonym of confidentiality concerning all client-bank matters; “Client confidentiality is very important for us and our customers (…) it is vital for ABC to prevent its products and services from being abused, while still respecting the privacy of its clients. In addition to adhering to local legislation, the bank applies strict Swiss regulations for the prevention of money laundering and terrorist financing in its international locations”

For the interviewed Corporate Privacy Officer of a multinational in The Netherlands privacy is a different issue than security: “There are significant differences (and overlaps) between security and privacy (multi disciplinary issue). Privacy is the result of a higher level of different business processes. Our corporation has a corporate privacy infrastructure in place: (…) a chief privacy officer plus a network of privacy officers throughout the worldwide company.” There are separate privacy procedures for customer and employee data: “We have a strategy on privacy for employee data, we have implemented binding corporate rules for employee data, is part of our ethics code. (…) For the consumer data (global privacy policy) there is a privacy policy for these data” “we have an extremely global centralized database on consumer data. Security is very strict and as well the access policy (…) There are very strict procedures and data are only available on a very limited basis. For outsiders if they want to use data, there are many elaborate privacy clauses in the contracts. (…) If the database would have a problem, the problem would be very big. Employees have to load consumer data in this database and aren’t allowed to keep it for themselves.”[39]. “We took the decision to encrypt all hard discs of our computers and laptops mandatory (…) We took the decision to do it everywhere not for the sake of privacy alone but also to avoid giving information about what security we use later (...). For encryption we built a strong business case based on avoiding risks because of US citizens’ personal data in the database”.

The Swiss bank the researcher interviewed stated that it has a continuous interest in offering clients products and services that are tailored to their needs. However, it is not currently considering PETs in their service offerings. While there is interest in PETs, but the drivers for adoption are based on the notion that: “PETs should enable us to do some kind of business. Of course it is interesting, it would remove the need for registration processes, it could be used in business relationship processes. But it is a long way, it is not just a technical issue, it is also a legal issue, regulatory issue. It is also a project feasibility issue, whether it can be made user friendly for the customer”.

The interviewed bank continuously reviews its product range and regularly assesses client satisfaction in key areas. When asked whether this is business potential for PETs for private banking customers with numbered account: “It depends on how many numbered accounts customers would want to use the Internet. We have internal systems where they are anonymized within our applications, and access is based on a need to know basis.” [39].

14. Three S-Curves

From the interviews can be deducted that when PET applications are purchased it isn’t for reasons of privacy protection but mostly it’s triggered by information security requirements. Most organizations that acquire PETs tools can be qualified as very mature organizations with regard to IAM processes. They all belong to the Top Class and Pro-Active maturity level. This is in line with the model shown in figure 8. The IAM processes follow a S-Curve as well. The same can be concluded for privacy protection. The CPO of the Dutch multinational said that “To align the different interests within our organization you have to look at the privacy maturity levels. For comparison we use the standard of the GAP Institute of Internal Auditors (GAP schema GTAG 5) [43]. “The GAP privacy level scheme follows a S-curve as well” [39].

The GAP GTAG 5 scheme is as follows:

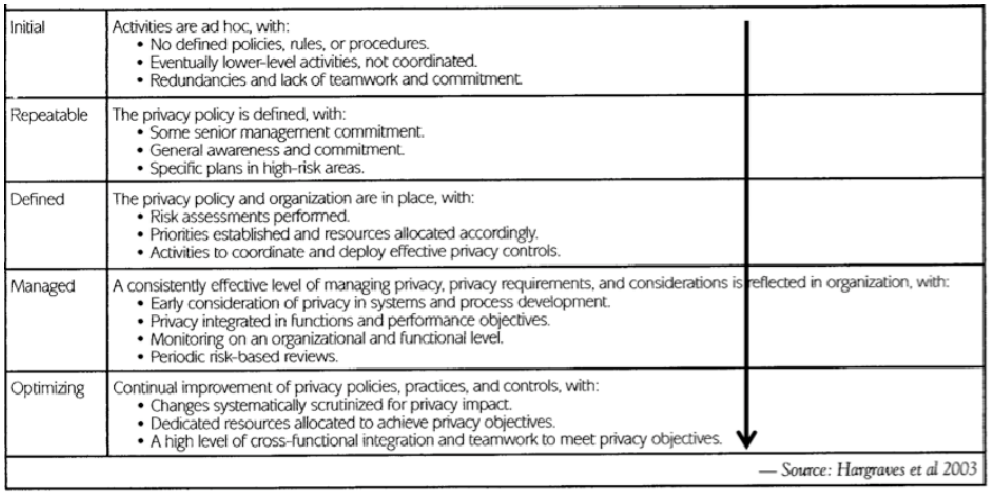


Figure 9 Processes in the development of privacy protection

The third S-curve is the PET adoption S-curve (see figure 1). The combination of the three S-curves leads to the figure 10 indicating a model of decision-making.

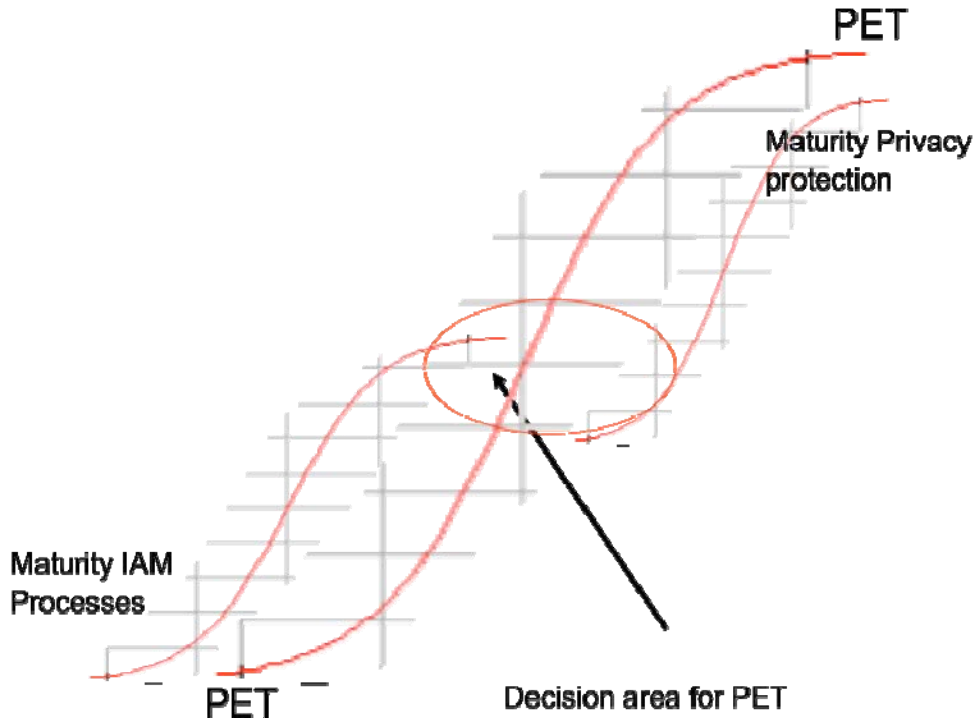


Figure 10 Three S-curves with decision area for PETs

These S-curves give an indication on which moment PETs could be introduced successfully into an organization as a means to protecting personal data.

15. Economic Justification for PETs

All persons interviewed consider potential damage to the brand and loss of business as the biggest risks of a privacy breach. Avoiding reputation damage in case of a breach is one of the biggest concerns. During the Bristol research workshops the comment was made that with regard to governmental organizations reputational damage seems not existent, as there isn't an alternative supplier (e.g. driving license fiasco at DVLA and the 25 million files lost by the IRS). The value of the brand (and the impact of a possible breach on it) is measured on a regular basis by many commercial organizations. Privacy is mostly seen as a negative driver (avoidance of breaches) in the business case, and not so much as positive driver (giving a market advantage). However management at the Dutch and Swedish multinational recognized the rising importance of privacy in sustainability reports (having eventually an effect on the cost of capital of the enterprise).

The interviewed Swiss bank applies standard IT risk management models such as Return on Security Investment (ROSI) when assessing potential damage and hence the security measures required per project. It is recognized that arriving at quantitative figures from empirical data is difficult, and fundamental questions remain as to how to value the protection of personal data: "How much would you pay as a customer for privacy protection? How much would you pay for example for protection of your health data?"

Perceptions with regard to the likelihood of a serious privacy incident vary. During the Bristol workshops, one of the participants reported that in his company in some cases privacy incidents are recorded and estimates of damage are provided. There is general awareness of potential risks like in the Norwich Union case where The Financial Services Authority (FSA) has fined Norwich Union Life £1.26 million for not having effective systems and controls in place to protect customers' confidential information and manage its financial crime risks.

A privacy incident at the Swiss bank in November 2000 lead to the unintended disclosure of about 100 customer files through the daemon account on their online banking site. It was potential reputational damage, as there were some VIPs involved. There was media exposure, and the threat that customers would withdraw their money and rumor about a run on the bank. That didn't happen. However it was not possible to quantify the costs and consequences of such an incident, either because such an exercise was not conducted, or because it went beyond the immediate response of how to recover from such an incident.

The commentary of the CPO of the Dutch multinational is remarkable in the sense that a serious privacy breach was never experienced, which was attributed to the existence of a thorough privacy infrastructure (encompassing various technical security measures). The likelihood of the occurrence of a privacy incident on a large scale is considered low (however of course not equal to zero) [39].

At the Swedish multinational (serious) breaches are experienced every couple of years; this type of risk is even expected to increase. In order to manage these risks better privacy impact assessments (PIA) are applied and risks are reported every year.

Developing an application like PETs in general, intended to protect a company to privacy and security breaches is fundamentally different from investments undertaken to automate the back-office to reduce expenses or increase capacity.

In almost all organizations the researchers investigated privacy protection is a strategic issue. Not so much to realize a competitive advantage, but as a competitive necessity. The brand or the reputation of the company is at stake, and if a serious breach happens everything will be done to prevent the breach to be published in the press. The potential impact that these breaches have on the strategic positioning of the organization should make them a concern of senior management. The question is how to evaluate PETs? How should a senior executive decide to invest in PETs?

In general evaluation of the effect of PETs on the company performance based on potential competitive impact is different from evaluation based on cost. The problem is that decision makers cannot predict the benefits accurately. Problem of investments in PETs is that costs are certain, however the benefits are absolutely uncertain. One is never sure of the benefits and quite sure of the costs. In fact the business case can be presented as an insurance premium against possible great losses. An important way to avoid the "trap of the negative net present value' is to analyze the business case of doing nothing, including the worst case scenario.

16. Conclusions

This paper points out that the adoption of PETs is problematic. There is only a limited use. The S-curves for IAM processes, the maturity of organizations, privacy protection and PETs give an explanation why PETs is taking off so slowly. Looking at the developed model (figure 3) those factors that are related to regulatory and legal compliance, to improved coordination and advice and information with regard to PETs, will to help to increase the deployment of PETs if these factors are stimulated. However there has to be also an economic justification for PETs and a method to quantify the benefits of a PETs investment. The answer to that problem is given in Privacy-Enhancing Identity Management in Business [35] and The Business Case for PET and the EuroPrise Seal [41].

References

[1] J. Bayer & N. Melone, “A Critique of Diffusion Theory as a Managerial Framework for Understanding Adoption of Software Engineering Innovations”, The Journal of Systems and Software, 1989/2, p. 161-166.

[2] R. Hes en J. Borking: Privacy Enhancing Technologies: the path to anonymity (revised edition), Report from the Dutch Data Protection Authority AV no 11 Den Haag: SDU, 2000.

[3] T.J. Cooke-Davies, Measuring Organizational maturity; Human Systems Limited; http://www.humansystems.net/papers/measuring_organizational_maturity.pdf; Last visited May 3, 2007

[4] Th.H. Davenport: Process Innovation – Reengineering work through Information Technology. Harvard Business School Press, 1993.

[5] G. de Roest, P. D. (2005). Een kwaliteitsbenadering voor blijvende effectiviteit van Security Management.

[6] J. Fagerberg ea, The Oxford Handbook of Innovation, New York: Oxford University Press, 2005.

[7] R.G. Fichman, "Information Technology Diffusion: A Review of Empirical Research," Proceedings of the Thirteenth International Conference on Information Systems (ICIS), Dallas, 1992, p. 195-206.

[8] R.G. Fichman, “The Diffusion and Assimilation of Information Technology Innovations”, in: R. W. Zmud ea, Framing the Domains of IT Management: Projecting the Future … Through the Past, Cincinnati: Pinnaflex Educational Resources, Inc., 2000.

[9] Forouzan, B; Business Data Communications; 2002; McGraw-Hill.

[10] T. Greenhalgh ea, “Diffusion of innovations in service organizations: Systematic review en recommendations”, The Milbank Quarterly, 2004/4, p. 581-629.

[11] B.H. Hall, “Innovation and diffusion”, In: J. Fagerberg ea, The Oxford Handbook of Innovation, New York: Oxford University Press, 2005.

[12] A. Jeyaraj, J.W. Rottman, M.C. Lacity, “A review of the predictors, linkages, and biases in IT innovation adoption research”, Journal of Information Technology, 2006/1, p. 1-23.

[13] KPMG Management Consulting; Groeimodel voor IV-functie – Het systematisch weergeven van een herinrichtingproces; December 2, 2001

[14] Koorn et al., Privacy Enhancing Technologies – Witboek voor beslissers; [.R. Koorn, H. van Gils, J. ter Hart, P. Overbeek, P. Tellegen, J. Borking]; Ministry of internal affairs and Kingdom relations; The Hague, 2004.

[15] A. Lam, "Organizational Innovation", In: J. Fagerberg ea, The Oxford Handbook of Innovation, New York: Oxford University Press, 2005.

[16] OECD Organization for Economic Co-operation and Development, Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd edition, 2005. Available at: http://www.oecd.org/

[17] M.A. Rivera & E.M. Rogers, "Evaluating public sector innovation in networks: extending the reach of the national cancer institute's web bases health communication intervention research initiative", The Innovation Journal: The public Sector Innovation Journal, 2004/9, p. 1-5.

[18] E.M. Rogers, Diffusion of Innovations, New York: Free Press, 2003.

[19] N. Smit; Erasmus University Rotterdam and Verdonck Kloosters and associates, Business Continuity Management – A maturity model; November 1, 2005.

[20] Stanford; Organizational Maturity Levels;

[21] http://www2.slac.stanford.edu/comp/winnt/system-administration/Organizational%20Maturity%20Levels.doc

[22] J. Tidd ea, Managing Innovation: Integrating Technological, Market and Organizational Change, Chichester: John Wiley & Sons, 2005.

[23] L. L. Tung & O. Rieck, "Adoption of electronic government services among business organizations in Singapore", Journal of Strategic Information Systems, 2005/14, p. 417-440.

[23] G.W. van Blarkom, J.J.Borking, J.G.E.Olk, Handbook of Privacy and Privacy-Enhancing Technologies, The Case of Intelligent Software Agents The Hague 2003 ISBN 90-74087-33-7, p. 22-30

[25] J. Vandecasteele, L. Moerland; Groeimodel voor IV-functie – Het systematisch weergeven van een herinrichtingproces; KPMG Management Consulting; Amsterdam, 2001.

[26] V. Venkatesh ea, "User Acceptance of Information Technology: Towards a Unified View", MIS Quarterly, 2003/3, p. 425-478.

[27] G. Zaltman ea, Innovations and organizations, New York: John Wiley & Sons Inc, 1973.

[29] http://www.prime-project.eu.org Privacy and Identity Management for Europe project number 507591

[30] H. van Rossum, H. Gardeniers, J.Borking, A. Cavoukian, J.Brans, N. Muttupulle, N. Magistrale, Privacy-Enhancing Technologies: The Path to Anonymity, A&V no 5a & 5b, Den Haag / Toronto 1995

[31] J.Borking, The Status of Privacy Enhancing Technologies, in E.Nardelli, S.Posadziejewsji &M.Talomo, Certification and Security in E-Services, Boston 2003, p.223

[32] J.Cas & Ch. Hafskjold, Access in ICT and Privacy in Europe, Experiences from technology assessment of ICT and Privacy in seven different European countries, Geneva 2006 p.41

[33] I.Leisner &J.Cas, Convenience in ICT and Privacy in Europe, Experiences from technology assessment of ICT and Privacy in seven different European countries, EPTA, Geneva 2006 p.50

[34] D.Sommer, The PRIME Architecture, in J.Camenish, R.Leenes & D.Sommer, Privacy and Identity Management for Europe, Brussels 2008, p.127

[35] A.Fairchild & P.Ribbers, Privacy-Enhancing Identity Management in Business, in Privacy and Identity Management for Europe, J.Camenish, R.Leenes & D.Sommer (eds.) Brussels, 2008 p. 69-100

[36] Tj.Bos, Adoptie van privacy-enhancing technologies bij publiekprivate instellingen (Adoption of privacy-enhancing technologies in public-private organizations, The Hague 2006

[37] V.H.Carr Jr, Technology Adoption and Diffusion, Montgomery (AL) 1996 http://www.au.af.mil/au/awc/awcgate/innovation/adoptiondiffusion.htm:

[38] J.J.Borking, Adoptie van online geschillenoplossing door organisaties, in P.van Schelven (ed.) (Adoption of online alternative dispute resolution by organizations, in From Dispute till Resolution) Deventer 2008

[39] P.Ribbers, A.Fairchild, J.Tseng, J.J.Borking, Extended Business Case Analysis, Brussels 2008

[40] G.Hosein, Privacy Process Requirements, PRIME F1, London 2007

[41] J.J.Borking, The Business Case for PET and the EuroPrise Seal, Kiel 2008

[42] A.van Eesteren & J.J.Borking, Lessons learned from the Europrise Certification, The Business View, Stockholm 2008. The EuroPrise project is subsidized by the EU Commission under the eTEN Programme. The EuroPrise project started op June 10 2007 and will continue till February 29 2009. See: http://www.european-privacy-seal.eu/about-europrise/fact-sheet

[43] U. Hahn, K.Askelson, R.Stiles, Managing and Auditing Privacy Risks, ltamonte Springs, Florida, 2008. See: http://www.theiia.org/guidance/technology/gtag/gtag5/

“Big brother on my desk” - Can office surveillance systems be compatible with privacy protection at the workplace? A question of legal clarity and corporate responsibility

Katja Stoppenbrink, LL.M., M.A.
Bad Neuenahr-Ahrweiler (Germany)
Katja.Stoppenbrink@ea-aw.de

Abstract:

“Microsoft seeks patent for office ‘spy’ software” – on January 16th 2008 this headline in the British newspaper The Times caused an outcry not only from civil liberties activists and privacy lawyers but also from trade unions and the general public. Two newsmen had in what seems to be a fair example of investigative journalism uncovered a document published by the US Patent and Trademark Office on December 27th 2007. They discovered that eighteen months before the software supplier had filed a patent application announcing the development of “a unique monitoring system” providing a human-machine interface for an ordinary office workplace of a hitherto unknown quality and degree of privacy invasiveness.

The envisaged computer system would allow employers not only to supervise their workers’ online communication, productivity and efficiency in terms of output per time unit, but henceforth managers could also monitor their employees’ performance by measuring their heart rate, galvanic skin response, brain signals, respiration rate, body temperature, blood pressure, their facial movements and expression. In addition an electromyograph could detect the electrical potential generated by their muscle cells. As stated in the application “[t]he system can also automatically detect frustration or stress in the user via physiological and environmental sensors” and thus “recognize an implicit need for assistance”. The apparent aim is to combine the management of “workflow around user activities” and monitoring group activity.

Against the backdrop of this prominent patent application I will explore the **challenges to workplace privacy** posed by the **combination of sensor and communication technology** in future activity-centric office surveillance systems. I will ask whether and how office surveillance systems can be (made) compatible with privacy protection at the workplace. To this end I will develop six hypotheses capturing the distinctive features of the **security vs. privacy dilemma in private contexts** as opposed to problems related to policing and/or the public sphere. The outcome is an attempt to strike a balance between conflicting privacy and security interests in employer-employee relations based on an adequate understanding of **legal requirements**, **business ethics and corporate responsibility**.

The six theses I intend to propound and substantiate are as follows:

1. The standard explication of the **security vs. privacy dilemma** does not adequately account for the peculiarities of private sphere phenomena such as **employer-employee relations** and has to be adjusted accordingly.

2. **Intra-corporate law enforcement and compliance** are distinct from and in some respects more difficult to achieve than law abidance in extra-corporate, public spheres (e.g. by means of traffic surveillance through closed circuit television). This applies to both security and privacy concerns. Proposed solutions have to be in line with other intra-corporate compliance schemes.

3. The **potential for privacy infringements** of a new generation of activity-centric office surveillance systems transgresses both a quantitative and a qualitative threshold. The development of such systems is **industry-driven** and irrespective of concerns for privacy and data protection management.

4. The legal landscape of privacy rights, data protection regulation and jurisprudence with respect to the workplace is fairly complex and detailed in some substantial and geographical areas and shows great blanks and lacunas in other areas. This **lack of legal clarity and accessibility of the law** favours ignorance of the respective legal framework by both employers and employees.

5. Legislation is required to decide on **criteria for workplace surveillance** such as the permitted degree of intrusiveness of novel techniques. The current debate (e.g. on the need for a special “employee data protection act” in Germany) focuses on the standard repertoire of criteria such as restrictions to the collection, storage, combination and disclosure of data gathered but also on issues such as notification requirements prior to surveillance, access conditions to sensitive personnel health data and genetic screening. Data protection management schemes should become an integral and legally required part of the implementation of office surveillance systems in privately owned companies.

6. Data protection and privacy legislation are substantiations of general legal and ethical principles. Intra-corporate employer-employee relations have so far been neglected in theory and practice of corporate responsibility. Whereas legislation is primarily of national origin, technology and growing awareness for corporate responsibility are – at least in the paradigm case of multinational corporations – worldwide phenomena. Global business ethical principles and corporate cultures may bridge the divide between national legislations. Privacy rights impact tests should thus become part of corporate self-regulation and be included in compliance schemes and certification processes.

References

Brown, David and Mostrous Alexi, Microsoft seeks patent for office ‘spy’ software, The Times, January 16, 2008 (retrieved January 17, 2008 from http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193480.ece).

Macbeth, Stephen W. et al. (Microsoft corporation), Monitoring group activities, United States Patent Application No. 20070300174, application date June 27, 2006, published December 27, 2007 US Patent and Trademark Office (retrieved January 17, 2008, from Patent Application Full Text and Image Database, http://appft1.uspto.gov/netahtml/PTO/search-adv.html).

Counter-Development – Technological Opposition as an Ethical Duty

Sandro Gaycken
Institut für Philosophie – Universität Stuttgart
sandro.gaycken@philo.uni-stuttgart.de

Abstract:

Resistance is an important measure for a society. It is a last means to access the social contract, the ultima ratio for cases of „tyranny“ when a ruler quits all commitments and ignores demands for a dismissal. To maintain this access thus is a necessary and ongoing task. Its foundations have to be secured continously. Judicial and ethical discussions as well as cultural practices aim at providing such foundations in legal and physical ways. Yet they rely on further basic conditions: To legally assess a political move, it has to be visible and understandable; and to physically engage political rulings, they have to have some physical dimension, a material outgrowth or representative. Since these are preliminary and necessary conditions they have to be reformulated as demands towards politics: political measures should be visibly, intelligibly and physically accessible. However, these demands are unlikely to be fulfilled by all politicians at all times. Some rather seem to prefer a certain inaccessibility of their ruling. Thus a society has to engage in a struggle for the maintaince of accessibility.

Up to this point, this struggle has not engaged the technical community. But this absence can not be continued. In the high tech age, politics start to develop substantial technological dimensions and the technical expert is needed to disentangle an ensuing and expanding net of political interests and technical functions in theoretical and practical ways.

My talk aims at developing this insight. To do so, first, resistance and its legal and practical foundations will be analysed, to recognise the underlying conditions of visible, intelligible and physical accessibility as demands towards political measures, followed by a brief look at the ensuing struggle. Next, after a look at technology and its potential to incorporate political interests, these conditions can be reformulated for cases of „political technologies“. Given these reformulations, the present high tech situation can be reviewed as discomforting: High tech entails structural features which demonstrate substantial inaccessibility. Thus finally, it can be concluded that the technical community has to engage in the quest for accessibility. It has to alert and enlighten the public about high tech-mediated inaccessibilities of politics and develop options to remove them. This specific and unique ethical duty will be termed counter-development and it will be suggested as an addendum to engineering and computer ethics.

Ethical aspects of information security

Elin Palm, PhD, Researcher
Division of Philosophy, The Royal Institute of Technology,Stockholm
elinpalm@infra.kth.se

Abstract:

Many efforts have been made to increase information security by furthering sound technology-based systems. This article however, examines the foundations for processing of personal data and information security from a social and ethical standpoint. Both data collection aiming at safety enhancement and protection of collected data are subjected to ethical analysis.

Paradoxically, various types of identity checks are used to enhance social safety at the same time as the personal data used for authentication/verification necessitates systems that guarantee safe storage thereof. Certainly, the increased processing of data has triggered debates on consequent privacy infringements and an uneven distribution of such invasions i.e. social sorting (cf. Gandy, 1993, Lyon, 2002). Still, several aspects are in need of further clarification. The contended view of this article is that in order to identify morally defensible ways of obtaining and securing personal data the following aspects (at least) must be investigated: (1) the purpose of data collection, (2) the type of data collected and the form of data collection and (3) the data subjects' possibilities of consenting to disclosure of personal data.

First, before addressing the frequently raised question: how much privacy are we willing to give up for a more secure life?, we should articulate what enhanced security means and under what conditions we have security. Moreover, security is often framed as a collective good vs the individual interest privacy and we are typically asked to accept the concrete and foreseeable increment of specific individuals' privacy for the possibility of increased security. This view however, should be contrasted with arguments to the effect that people have a shared interest in privacy and that privacy is socially valuable (Regan, 1995:213).

Second; what types of information are privacy sensitive and why? A brief survey of prevailing privacy protection legislation gives that the type that enjoys protection is most often of an obviously sensitive kind e.g. information about sexual orientation, political and/or religious views, leaving aside information that may become privacy sensitive in certain contexts. Drawing on the reasoning of Helen Nissenbaum's reasoning (Nissenbaum, 1998, 2003) a contextual approach on privacy sensitive data is suggested. Arguably, particular conditions, contexts and the purpose behind data collection may influence individuals' perception of data collection. Other factors that are likely influence whether and to what degree individuals consider certain information or ways of processing data privacy sensitive are: sex, ethnicity.

Third, the conditions under which individuals can be said to, in a substantial way, approve of or consent to having their personal data processed (collected, processed, stored, transferred) should be investigated. The principle "informed consent" will be borrowed from medical ethics in order to spell out conditions under which individuals consent to disclosure of personal data can be considered morally justifiable.

This discussion is intended as a probe for fair conditions of data collection and information security.

Law, justice and ethics for preemptive security practices[1]

Gloria González Fuster
Institute for European Studies (IES) /Research Group on Law Science Technology & Society (LSTS), Vrije Universiteit Brussel (VUB)
Gloria.Gonzalez.Fuster@vub.ac.be

1. Introduction

The current evolution of security practices is marked by a global trend towards pre-emption, in which predictive data mining and profiling techniques are playing an increasingly prominent role. Do evolving security practices represent specific new challenges for law, ethics and justice, requiring ad-hoc legal responses? Discussing a possible answer to this question, the present paper first explores the essential features of such practices as currently developed in the name of security. Second, it examines the possible need to reframe the right to data protection in the light of such developments, and the eventual need for other legal responses.

2. The specificity of contemporary preemptive security practices

Since September 9, 2001, preemption has progressively become an essential feature of many security strategies around the world. The rationale behind such forward-looking strategies is the alleged need to anticipate the manifestation of certain events (particularly terrorist events), in the belief that reaction *a posteriori* might be impossible, or unsatisfactory. Applying the logic of preemption in the field of terrorism and crime fighting can however by itself tend to contradict certain traditional basic principles of criminal law, and particularly the presumption of innocence, according to which nobody can be considered guilty of having committed an offense before it is proven that they have committed such an offence. Preemption in its purest form should, on the contrary, aim at the identification of offenders before they are able to commit any offence. This is not, however, the only potential conflict of such practices with individuals' rights.

2.1. A description

Preemptive security practices tend currently to be deployed in many different areas, and through different strategies. They can rely on different degrees of anticipation. A first group of practices is based on the verified existence of a concrete threat. They are aimed at foreseeing the materialisation of a known danger in time to avoid any harm; they focus, for instance, on locating and stopping a suspected individual. A second group of practices aims at assessing the

[1] This paper is partially inspired by "The role of law, ethics and justice in security practices", a statement submitted jointly by Gloria González Fuster, Serge Gutwirth and Paul de Hert to the *Security: Advancing a Framework for Enquiry (SAFE): A Forward Look* workshop held on March 10-11, 2008 at the International Peace Research Institute (PRIO) (Oslo).

risk of appearance of unexpected threats. In these situations there are no suspects, nor even threats (yet), but simply a belief according to which threats might appear (eventually).

A third group of practices, which can be conceptually situated between the two already mentioned, takes as a starting point the belief in the existence of a diffuse threat. The objective of these practices is to refine/define more 'concrete' threats, and possibly, at a later stage, to identify individuals potentially embodying such threats. These practices generally rely on the use of predictive data mining and profiling, and are developed in two distinct steps. Firstly, based on massive data processing, are constructed criteria and categories to which different levels of 'risk' are attributed. This is done using data mining techniques that allow determining patterns of 'suspect behaviour', and defining accordingly 'risky groups'. Secondly, and again through massive processing of data, individuals matching the profile of the 'suspected categories' are sought after. Those matching the profile will be considered 'suspect', or 'worth further examination' or 'attention'.

As in order to determine that certain individuals are to be considered 'worth further examination' their data is correlated to an abstract description of suspicious profiles, these processes have been described as relying on 'categories of suspicion'.[2] This term illustrates one of the most relevant issues related to these practices from the point of view of law and justice, i.e. the fact that the attribution of 'suspicion' to individuals takes place indirectly. Those considered as suspicious are not considered so because of a specific link between their personal behaviour and certain activities, but because their data matches the general profile attributed (via data mining) to those allegedly involved in certain activities considered as indicators of threats.[3]

In this context, profiling can be described as the determination of characteristics or combinations of characteristics that might lead to identify someone or something as potentially worth investigation, and data mining as the use of advanced algorithms to trawl through databases to discover someone or something matching that profile.[4] However, more commonly data mining generally refers both to the construction of profiles and the search for those matching the profiles. In practice, moreover, the different logical steps tend to blur, and ideally the construction of profiles is to be constantly readjusted, taking into account in real time the results that the application of the obtained profiles is providing.

Preemptive security practices relying on abstract 'categories of suspicion' generally share a series of common features. First, they are dependent on the processing of massive quantities of data, which can either be collected especially for such purposes or, much more often, be re-used after having been collected for other, totally unrelated purposes (for instance, in the context of commercial activities). Second, the practices rely on the use of different technologies, including various information and communication technologies. Third, they are inscribed in a

---

[2] Expression originally phrased by Gary T. Marx (for a discussion, see: Lyon, David (ed.) (2007), *Surveillance Studies: An Overview*, Polity Press, Cambridge, p. 21 and p. 198).

[3] Levi, Michael and David S. Wall (2004), "Technologies, Security and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, 31(2), June, p. 199. See also: Crossman, Gareth (2008), "Nothing to hide, nothing to fear?", *International Review of Law, Computers & Technology*, 22(1-2), March-July, p. 118.

[4] House Of Lords European Committee (2007), *The EU/US Passenger Name Record (PNR) Agreement*, Report with Evidence, HL Paper 108, 21st Report of Session 2006-07, The Stationary Office Limited, London, 5 June, p. 10. For a description of profiling and data mining, see also: Dinant, Jean-Marc, Christophe Lazaro, Yves Poullet, Nathalie Lefever and Antoinette Rouvroy (2008), *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, January 11.

general policy dynamic; they do not appear and cannot be implemented on their own. They are an element in a general trend marked by other policy decisions such as the promotion of networking of data controllers, of information sharing, or of rendering interoperable certain independent databases. Any measure that might help to increase the quantity of data available is in principle a potentially positive contribution to the use of predictive data mining.

The tendency to collect and process increased quantities of data can be described as a 'renewed panopticism', underlining the idea that profiling attempts to encompass the whole population.[5] Some authors, however, have highlighted that even if the whole population might be affected, the main effect of these techniques is to differentiate between groups of people, sorting out individuals and placing some of them in a less privileged position than others.[6] Predictive data mining does not simply require the processing of everybody's personal data as if everybody was a potential suspect, it is also directed towards the delimitation of minorities to be regarded as more suspicious than the rest.

2.2. Concrete examples from the US and the EU

In the United States (US), a report to the US Congress of the Office of the Director of National Intelligence provided in February 2008 an interesting overview of US intelligence data mining development programs. Data mining as described in the report is the technique used by intelligence agencies to search through databases in order to discern patterns of activity that could indicate a threat to national security, or, in other terms, to discover or locate "*a predictive pattern or anomaly indicative of terrorist or criminal activity*".[7] Data mining-related intelligence projects described in the document include for instance the Video Analysis and Content Extraction (VACE) project, which seeks to automate the process of reviewing video looking for content potentially of intelligence value. A more original project is Reynard, which officially seeks to study the emerging phenomenon of social and 'particularly terrorist' dynamics in virtual worlds and large-scale online games and their (eventual) implications for the intelligence community. Other research projects are more general in scope, for instance aiming to refine methodologies that would allow for the constant assessment of threats to eventually determine "*the threat likelihood of unexpected threat entities*".[8]

It has been much discussed whether the European Union (EU) has adopted the US approach to security through preemption or not.[9] Even if predictive data mining for security purposes was supported only by the US, the impact of such measures could be considered highly relevant also for EU citizens, especially inasmuch certain practices are deployed in the US allowing for the processing of data related to EU citizens; for instance, in the context of official or un-official use of Passenger Name Record (PNR) data for data mining and profiling by US authorities.[10]

---

[5] Aradau, Claudia and Rens Van Munster (2007) "Governing Terrorism through Risk: taking precautions, (un)knowing the future", *European Journal of International Relations*, 13(1), p. 104.
[6] Lyon, David (ed.) (2007), *Surveillance Studies: An Overview*, Polity Press, Cambridge, p. 115.
[7] Office Of The Director Of National Intelligence (2008), *Data mining report*, February 15, p. 1.
[8] Office Of The Director Of National Intelligence (2008), *Data mining report*, February 15, p. 4.
[9] For a positive answer to the question, see: De Goede, Marieke (2008), "The Politics of Preemption and the War on Terror in Europe", *European Journal of International Relations*, 14, p. 162.
[10] Privacy International (2004), *Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection*, First Report on 'Towards an International Infrastructure for Surveillance of Movement', February, pp. 9-10.

Some developments seem to support the idea that the EU is also open or at least not fully reluctant to the implementation of this kind of practices, and/or is at least favouring the deployment of the enabling conditions that would allow for such practices to develop. Certain measures already adopted by the EU legislator go in the direction of allowing for the massive retention and eventual use for law enforcement purposes of data not originally collected for such purposes, such as the Data Retention Directive.[11] EU institutions have also regularly backed up decisions encouraging various levels of information sharing. A more concrete step towards pre-emption can be seen in the 3rd Money Laundering Directive, in which appears an explicit reference to the need to provide a 'preventive effort' against money laundering.[12]

The current proposal for a PNR EU-system provides probably the best illustration of EU support of predictive data mining in a security context. The European Commission presented a proposal for a Framework Decision on the use of PNR for law enforcement purposes on November 6, 2007.[13] The proposal prescribes obligations relating to the handling of PNR data to be undertaken by the Member States in relation to air carriers operating flights to or from the territory of one or more of the Member States. Under the scheme proposed, airlines should keep collecting passenger data for commercial purposes as usual, and Member States would designate Passenger Information Units to collect the PNR data from the airlines. The Passenger Information Units should carry out risk assessments of passengers "*in accordance with criteria and guarantees provided for under national law*" (in other words, 'to be determined').

Data would be processed for the purposes of preventing or combating terrorism or organised crime, including, in practice, to identify persons or their associates who may be involved in such offences, but also to update 'risk indicators'. All passengers would be assessed through such 'risk indicators'. Depending on the results of the assessment, there are two main perspectives for passengers: first, that they fall under the 'high risk' category, which would qualify them for extra inspection;[14] second, that they do not fall under any 'high risk' category, which would not qualify them to ask for the data about them to be removed from the system, but would keep them under the 'normal surveillance' regime, as the data already processed would anyway be retained and used for further data mining and profiling. The proposed PNR system therefore uses data from the totality of the population involved (in this case, all those booking a flight for the routes concerned) in order to firstly determine/discover/establish what a 'suspect' might look like, and, secondly, in order to place under extra-surveillance those resembling the abstract profile of a suspect.

---

[11] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ, L 105, 13.4.2006, pp. 54-63.

[12] Recital (1) of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ, L 309, 25.11.2005, pp. 15–36.

[13] European Commission (EC) (2007), *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, 6 November, Brussels. The background of the measure includes the invitation launched in March 2004 by the Council to the EC to bring forward a proposal for a common EU approach to the use of passenger data for law enforcement purposes. The Hague Programme also invited the EC to act in this direction.

[14] "*The rationale behind identifying unknown high-risk passengers is that this allows for secondary screening upon their arrival and further questioning by security officers and in specific circumstances, in combination with other information, to a refusal of entry in the territory of the destination country*" [European Commission (2007), *Accompanying document to the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes: Summary of the Impact Assessment*, Commission Staff Working Document, SEC(2007) 1422, Brussels, p. 3].

2. Impact and possible responses

The impact on privacy and civil liberties of the use of predictive data mining for security purposes is widely acknowledged. Because of such impact, the US Intelligence Advanced Research Projects Agency (IARPA) is for instance investing in projects that develop ad-hoc privacy protecting technologies. However, the repercussions for individuals' rights might be much wider than the effects potentially countered by any ad-hoc technologies.

One of the main ethical issues at stake in the deployment of these practices is related to the co-option of the entire population (or the entire 'relevant corpus') into the construction of 'categories of suspicion'. The data used to determine through data mining 'who' and 'what' is to be considered 'worth special attention' is directly taken from the normal, daily life of the population explored, which is given no other choice than to provide the data and accept the inferences that will be made on its basis. 'Normal' lives are scrutinized to obtain a more refined definition of what does 'normal' exactly mean, in the belief that the minority leading 'not so normal' lives deserves to be placed under reinforced surveillance. Indirectly, everybody is co-opted into incriminating the other.

From the perspective of justice, a key issue is the problem of discrimination. This problem can manifest mainly in two ways: first, discrimination can directly take place during the construction of profiles; second, discrimination is inevitably the result of the practice itself. Discrimination in the first sense has been particularly explored, especially as some counter-terrorist data mining and profiling programs have been believed to incorporate ethnic and religious indicators. As the use of such indicators reinforces the degrading impact of security practices,[15] calls have been voiced out for so-called 'neutral' profiling, notably preferring the use as indicators of behavioural characteristics, which are believed to allow for 'neutral profiling', at least insofar these indicators are implemented 'in a neutral manner' and not used as mere proxies for ethnicity, national origin or religion.[16] The question arises, however, whether any indicators can be used 'in a neutral manner' for practices such as data mining and profiling that have as main aim to differentiate, to sort out, to categorise and, therefore, to discriminate. It might actually be argued that indicators that fail to discriminate between individuals are simply to be considered invalid indicators: profiling requires inevitably discriminating variables, and discriminating results.

To this fundamental problem needs to be added another caveat, related to the conditions in which data mining and profiling techniques are implemented, notably the quantity and quality of data available on different categories of individuals. The most fundamental question might however be related to the legitimacy of the power for the definition of relevant categories. Some consider a priority to explore who is responsible for their definition.[17] Others have called

---

[15] It has been shown that profiling practices have a more serious impact than 'neutral' law enforcement methods. While anyone stopped, searched or questioned by the police may feel intimidated or degraded to a certain extent, the encounter has a particularly humiliating effect when the characteristics such as race or religion play a role in the law enforcement officer's decision (Moeckli, Daniel (2006), "Terrorist Profiling and the Importance of a Proactive Approach to Human Rights Protection", December 16 (retrieved from: http://ssrn.com/abstract=952163), p. 19).

[16] Scheinin, Martin (2007), *Summary of the Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Advanced Edited Version, A/HRC/4/26, January 29, p. 16.

[17] Lyon, David (ed.) (2007), Surveillance Studies: An Overview, Polity Press, Cambridge, p. 185-186.

for a better assessment of the techniques themselves.[18] There have been also calls for a more specific regulation of profiling.[19]

2.1. Re-framing data protection?

The legal response to counter the negative impact of preemptive security practices is often constructed in terms of anti-surveillance, emphasising the role to be played by the right to privacy and the right to data protection. Both rights as currently configured in the EU surely have a very important role to play in the context of these practices. But does the current legal framework provide for an effective response to the identified challenges?

The right to privacy and the right to the protection of personal data are recognised at the highest level in the EU in the Charter of Fundamental Rights,[20] which establishes them as separate rights, in Article 7 and Article 8. They have been described as having distinct roles to play.[21] Whereas to the right to privacy is basically oriented towards a negative protection, prohibiting undue interferences with a space considered 'private', the right to the protection of personal data has been traditionally configured as a 'positive' right, granting the individual a series of specific positive rights related to their own personal data, based on a series of established principles. Systems like the proposed EU-PNR system, or any other massive processing of personal data, involve numerous and important issues related to existing data protection law.[22] In the context of data protection, profiling is generally dealt with through provisions establishing some safeguards against automated decision-making, not always with convincing and effective results.[23]

Present-day predictive data mining practices could call for critical reconsideration of certain traditional principles of data protection, and in particular the role to be played by the principle of 'data quality', as well as its correlated subjective right of 'rectification'. The right to the protection of personal data as established in the Charter mentions the right of data subjects to access their data, and to have it 'rectified': by virtue of Article 8(2) of the Charter, "*[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified"*. The recognition of a right to render personal data accurate, without a

---

[18] European Data Protection Supervisor (EDPS) (2007) *Opinion on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 20 December, Brussels, p. 6.

[19] Weitzner, Daniel J. et al. (2006), *Transparent Accountable Data Mining: New Strategies for Privacy Protection*, Computer Science and Artificial Intelligence Laboratory Technical Report, MIT, January 27, p. 9.

[20] *Charter of Fundamental Rights of the European Union*, Official Journal of the European Communities, C 364, 18.12.2000, pp. 1-22.

[21] See, notably: De Hert, Paul and Serge Gutwirth (2003), "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location based services and the virtual residence" In I. f. P. T. Studies (Ed.), *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview: Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)*.

[22] See, in this sense: Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data And Working Party On Police And Justice (2007), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007*, WP145, WPPJ 01:07, December.

[23] For instance, in Art. 15 of the Data Protection Directive (Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50). France has had legislation dealing with this topic since 1978. The original EC proposal for a Directive on telecommunications and privacy contained a provision dealing with the creation of electronic subscriber profiles, but the provision was deleted from later drafts (Bygrave, Lee A. (2002), *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague, London, New York, p. 320). The EU legislator has insofar failed to provide a fully satisfactory response to the issue of profiling through the regulation of automated decision-making.

parallel right to transform such data into inaccurate data,[24] presupposes that it is always advantageous for the individuals for data about them to be as accurate as possible. Many consider the 'data quality' principle especially relevant precisely in the context of data mining, and it is common to relate certain difficulties for the widespread implementation of security practices to insufficiencies of data quality,[25] or even assert that poor quality of data is the major obstacle to the effective deployment of preemptive security practices.

These assumption need to be critically questioned. Ultimately they can be interpreted as implying that 'perfect quality of data' could lead to perfect effectiveness of predictive data mining for security purposes, which is to say the least unclear. Moreover, recognising in practice a wider degree of freedom for the data subject to adjust the level data quality of their data (for instance, in the light of the explicitly foreseen purposes of processing) would actually be more consistent with nowadays interpretations of the right to data protection in terms of positive user control. This view, which can be seen as an attempt to conceptualise the right to data protection as a positive freedom with respect to identity, links the right to data protection to the free determination of how persons positively want to be represented.[26] Acknowledging a right to freely determine the accuracy of personal data would be a more logical step into the construction of real user control, but could also grant to the data subjects the opportunity to make real ethical choices on whether to accept or not the processing of their data for the systematic incrimination of certain minorities.

2.2. Towards the 'rights of suspected categories'

The impact on society of preemptive security practices is not limited to issues of privacy and data protection. Civil liberties concerns related to the use of data mining and profiling for criminal purposes have been notably described in reference to the presumption of innocence, search and seizure, due process (the right to view, challenge and refute information before a formal decision is made), equal protection, and fair and public trial.[27] Coming back to the notion of 'categories of suspicion', it can be asserted that whereas, on the one hand, the right to privacy and the right to data protection need to offer an effective protection for all those whose private lives are interfered with, and all those whose personal data is used for the construction of such 'categories', on the other hand the law needs to provide also special, enhanced protection to those (rightly or wrongly) identified as falling under a 'category of suspicion'.

Suspects have traditionally been granted special rights to compensate for the special position they are placed in when considered as such by the authorities. If the legislator decides to treat as 'suspects' (or as persons 'worth further attention') entire groups of individuals simply

---

[24] The absence of a right to un-rectify data does not imply that current EU law leaves unprotected inaccurate personal data, which are still to be considered personal data (Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (2007), *Opinion 4/2007 on the concept of personal data*, Adopted on 20th June, WP136, 01248/07/EN, p. 6).

[25] See, for instance: Levi, Michael and David S. Wall (2004), "Technologies, Security and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, 31(2), June, p. 194; EC (2005), *Impact Assessment Annex to the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, Commission Staff Working Document, COM(2005) 475 final, 4.10.2005, p. 2.

[26] Van Den Hoven, Jeroen (ed.) (2005), *Managing Identity, Privacy & Profiles*, Alter Ego Deliverable 1.3, SOTA Delft Technical University, May 25, p. 47.

[27] Cavoukian, Ann (2003), *National Security in a Post-9/11 World: The Rise of Surveillance… the Demise of Privacy*?, Green College, University of British Columbia, May, pp. 32-35.

because they match or seem to match a statistical definition of a 'suspect' or of a 'worth further attention' person, it should also provide to those groups accordingly protective rights.

The substantive content of such 'rights of suspected categories' could find its roots in the doctrine of the rule of law, supporting the protection of the individual through the provision of open and clear laws, and giving special consideration to equality and due process, including the principles of fair trial and the presumption of innocence, among others. To elaborate the minimal requirements for the protection of those falling under suspected categories it could also be especially useful to take into account the recent and soon-to-come European case law on terror blacklisting, in particular as established by the European Court of Justice (ECJ). Due process requirements related to data mining and profiling practices oblige to consider carefully issues of transparency and accountability of these practices: the techniques implemented should be transparent enough as to allow for judicial review not only of the data used, but also on the logic applied to process the data. Finally, systems like the proposed EU-PNR system, in which the 'categories of suspicion' could allow for a very large number of passengers to be erroneously identified as potential high-risk passengers, should include specially designed measures. The 'rights of the alleged high-risk passenger' shall include notably provisions on redress and compensation.[28]

3. Conclusions

Exploring profiling and predictive data mining in the context of preemptive security practices has lead to assert that the response needed to frame their negative impact on ethics and justice clearly goes beyond the agenda of privacy advocacy. Moreover, the response might actually require the re-thinking of certain fundamental assumptions of data protection law, such an excessive reliance on the virtues of the 'data quality' principle.

The paper has taken the proposed EU PNR-system as an example for discussion. The EC has already announced that it will follow closely the developments of such EU-PNR system to take them into account in order to prepare future proposals for the management of external borders,[29] offering to the European Data Protection Supervisor (EDPS) the opportunity to underline that recent EC's proposals on border management "*are part of a long series of proposals or measures intended to process data about innocent individuals. A broad reflection about this kind of proactive surveillance and its real usefulness in the fight against terrorism should be encouraged*".[30] Hopefully such a reflection will take into consideration that citizens shall be given the opportunity to determine which data about them is processed, and how, not only because such processing determines how they are personally to be represented, but also

---

[28] In this sense, González Fuster, Gloria and Paul De Hert (2007), "PNR and compensation", in Lodge, Juliet (ed.) (2007), *Are You Who You Say You Are? The EU and Biometric Borders*, Wolf Legal Publishers, Nijmegen, pp. 101-109.

[29] EC (2008), *Communication from the Commission to the European Parliament and to the Council on an entry/exit system at the external borders of the European Union, facilitating of border crossing for* bona fide *travellers, and an electronic travel authorisation system*, COM(2008)final, Brussels, p. 8.

[30] European Data Protection Supervisor (EDPS) (2008), *Preliminary Comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union" COM(2008) 69 final, the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Examining the creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final, and the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final*, March 3, Brussels, p. 7.

because it determines their contribution to how the others are represented, categorised and treated.

4. References

Aradau, Claudia and Rens Van Munster (2007) “Governing Terrorism through Risk: taking precautions, (un)knowing the future”, *European Journal of International Relations*, 13(1), pp. 89-115.

Bygrave, Lee A. (2002), *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague, London, New York.

Cavoukian, Ann (2003), *National Security in a Post-9/11 World: The Rise of Surveillance… the Demise of Privacy?*, Green College, University of British Columbia, May.

Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, C 364, 18.12.2000, pp. 1-22.

Crossman, Gareth (2008), “Nothing to hide, nothing to fear?”, *International Review of Law, Computers & Technology*, 22(1-2), March-July, p. 118.

De Goede, Marieke (2008), “The Politics of Preemption and the War on Terror in Europe”, *European Journal of International Relations*, 14, pp. 161-184.

De Hert, Paul and Serge Gutwirth (2003), "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location based services and the virtual residence" In I. f. P. T. Studies (Ed.), *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview: Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)*.

Dinant, Jean-Marc, Christophe Lazaro, Yves Poullet, Nathalie Lefever and Antoinette Rouvroy (2008), *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, January 11.

Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, Official Journal of the European Union, L 309, 25/11/2005, pp. 15–36.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available

electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union, L 105, 13.4.2006, pp. 54-63.

European Commission (EC) (2005), *Impact Assessment Annex to the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, Commission Staff Working Document, COM(2005) 475 final, 4.10.2005.

--- (2007), *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, 6 November, Brussels.

--- (2008), *Communication from the Commission to the European Parliament and to the Council on an entry/exit system at the external borders of the European Union, facilitating of border crossing for* bona fide *travellers, and an electronic travel authorisation system*, COM(2008)final, Brussels,

European Data Protection Supervisor (EDPS) (2007) *Opinion on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 20 December, Brussels.

--- (2008), *Preliminary Comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union" COM(2008) 69 final, the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Examining the creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final, and the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final*, March 3, Brussels.

González Fuster, Gloria and Paul De Hert (2007), "PNR and compensation", in LODGE, J. (ed.) (2007), *Are You Who You Say You Are? The EU and Biometric Borders*, Wolf Legal Publishers, Nijmegen, pp. 101-109.

House Of Lords European Committee (2007), *The EU/US Passenger Name Record (PNR) Agreement*, Report with Evidence, HL Paper 108, 21st Report of Session 2006-07, The Stationary Office Limited: London, June 5.

Levi, Michael and David S. Wall (2004), "Technologies, Security and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, 31(2), June, pp. 194-220.

Lyon, David (ed.) (2007), *Surveillance Studies: An Overview*, Cambridge: Polity Press.

Moeckli, Daniel (2006), "Terrorist Profiling and the Importance of a Proactive Approach to Human Rights Protection", December 16, retrieved from: http://ssrn.com/abstract=952163.

Office Of The Director Of National Intelligence (2008), *Data mining report*, February 15.

Privacy International (2004), *Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection*, First Report on 'Towards an International Infrastructure for Surveillance of Movement', February.

Scheinin, Martin (2007), *Summary of the Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Advanced Edited Version, A/HRC/4/26, January 29.

Van Den Hoven, Jeroen (ed.) (2005), *Managing Identity, Privacy & Profiles*, Alter Ego Deliverable 1.3, SOTA Delft Technical University, May 25.

Weitzner, Daniel J. et al. (2006), *Transparent Accountable Data Mining: New Strategies for Privacy Protection*, Computer Science and Artificial Intelligence Laboratory Technical Report, MIT, January 27.

Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data (2007), *Opinion 4/2007 on the concept of personal data*, Adopted on 20th June, WP136, 01248/07/EN.

Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data And Working Party On Police And Justice (2007), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007*, WP145, WPPJ 01:07, December.

Concepts of Privacy-Enhancing Identity Management for Privacy-Enhancing Security Technologies

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein, Germany

Abstract:

Security as well as privacy is a need of society and its individual members. When designing security technologies, both goals should be taken into account. Designing security technologies without keeping privacy requirements in mind may result in systems which create additional risks to society and where side-effects are difficult to control. When the identification or surveillance of individuals is necessary from the security point of view, the used approaches should be limited to single, specified cases. This text shows how building blocks of privacy-enhancing identity management can contribute to integrate privacy objectives into security technologies. Thereby it clarifies that the goals are not in all cases antagonistic, but may constitute a large overlap, e.g., when preventing misuse beforehand or providing fair information to all parties concerned. This is not only necessary because of individual privacy needs, but also to protect economic interests.

1. Introduction

According to Maslow's hierarchy of needs (Maslow 1943), safety and security are quite important requirements for individuals' lives. The same is true for society as such. National states as well as state unions strive for keeping a high level of safety and security – to achieve and keep stability of their own governmental, economic and societal system constituted by their citizens. Security technologies are meant to support this aim and in particular to prevent and possibly counter attacks and threats concerning security. The field of security technologies encompasses so different approaches as private alarm systems, virus protection systems for personal computers, surveillance systems, border control systems or international police co-operation systems.

Especially the terroristic attacks of September 11, 2001 in the United States of America boosted development and use of security technologies, also in the European Union. It should go without saying that other needs of society and basic rights of individuals must not be neglected when researching, designing, implementing or using security technologies. A prominent basic right is the right to privacy.

This text shows how privacy-enhancing technologies, taking the example of user-controlled, data minimising identity management, can help to prevent security-relevant attacks and threats and thereby contribute to privacy-compliant or even privacy-enhancing security technologies. The following parts are organised as follows: The melange of different security objectives which sets the scope for this text is explained in chapter 2. In chapter 3 important building blocks of privacy-enhancing identity management are introduced. They are evaluated with

respect to possible applicability in security technologies in chapter 4. Finally chapter 5 presents a conclusion.

2. Melange of Security Objectives

Obviously there are various ways to prevent or counter threats to society's security which work alone or in combination:

1. Preventing threats:
   In several scenarios, threats can be prevented altogether, e.g., if intended or unintended misuse or direct attacks simply cannot be performed. In information and communication technologies (ICT) appropriate system design could often make sure that usage is restricted to predefined, desired purposes and actions. In general, this is easier to implement in closed systems with a limited scope than in open, multi-purpose systems.

2. Limiting the effects of threats:
   In some cases, threats cannot be prevented, but their effects can be limited to a degree tolerable to society. There might be ways to deal with the effects, e.g., a functioning legal system or insurances.

3. Detecting threats and criminals responsible for threats:
   If threats cannot be prevented, it is good to detect them in an early stage and take measures to counter them. Also the actors responsible for the threats could be singularised in the population so that they can be arrested or that the effects of the threats may be minimised.

4. Arresting criminals:
   If the criminals can be arrested, the legal system of trials and sentencing comes into place in order to prevent any other harm stemming from the perpetrator and to deter others from becoming a criminal themselves.

In all cases undesired side-effects should be avoided, such as, e.g., arresting and sentencing the wrong persons, intimidating unsuspicious people or even creating a bigger risk to society by the measures taken. Such a risk may be a loss or significant reduction of citizens' trust in society or in the legal system, another kind of risk can be a vulnerability for attacks, e.g., via backdoors in ICT systems, via single points of failure or via accumulation of interesting data which are hard to secure. For example, mass surveillance is worse (both for those who are unjustifiably under surveillance and for those having to do the surveillance) than an effective supervision of individuals and small groups. For that reason, procedures and methods for the latter precisely tailored supervision which do not scale to allow mass surveillance should be preferred over others (cf. Pfitzmann, Köhntopp 2001).

In the ICT world, accountability of users and actions is an important ICT security goal because users who can be held accountable for their actions usually do not misuse the system. All the same, privacy of users, e.g., via the ICT security goals of anonymity or unlinkability, is also important because it is an important basis for the individuals' personalities and honest acting as demanded in many democratic processes. A big part of the population is aware of their need of privacy (cf. Eurobarometer 2008). Several ICT concepts show that privacy of users can be

maintained while also achieving accountability or while preventing misuse altogether (e.g., Chaum 1985 or Pfitzmann, Waidner, Pfitzmann 2000).

3. Concepts of Privacy-Enhancing Identity Management

Privacy-enhancing technologies – also "privacy technologies – have been discussed since about three decades (cf. Chaum 1981, Chaum 1985). Many concepts and tools can be used in privacy-enhancing identity management (cf. Hansen 2008b): As not all of one's so-called partial identities and attributes (see Figure 1) are relevant in each individual context, individuals should only disclose the necessary extent of data and separate the contexts from each other (cf. Clauß, Köhntopp 2001). In the physical world of face-to-face meetings this is done intuitively; in the ICT world people need technical support, the more so as it cannot be assumed that disclosed data – including data trail users are not aware of – will be deleted or "forgotten" after some time or that the data, possibly from different contexts, won't be linked and analysed later on.

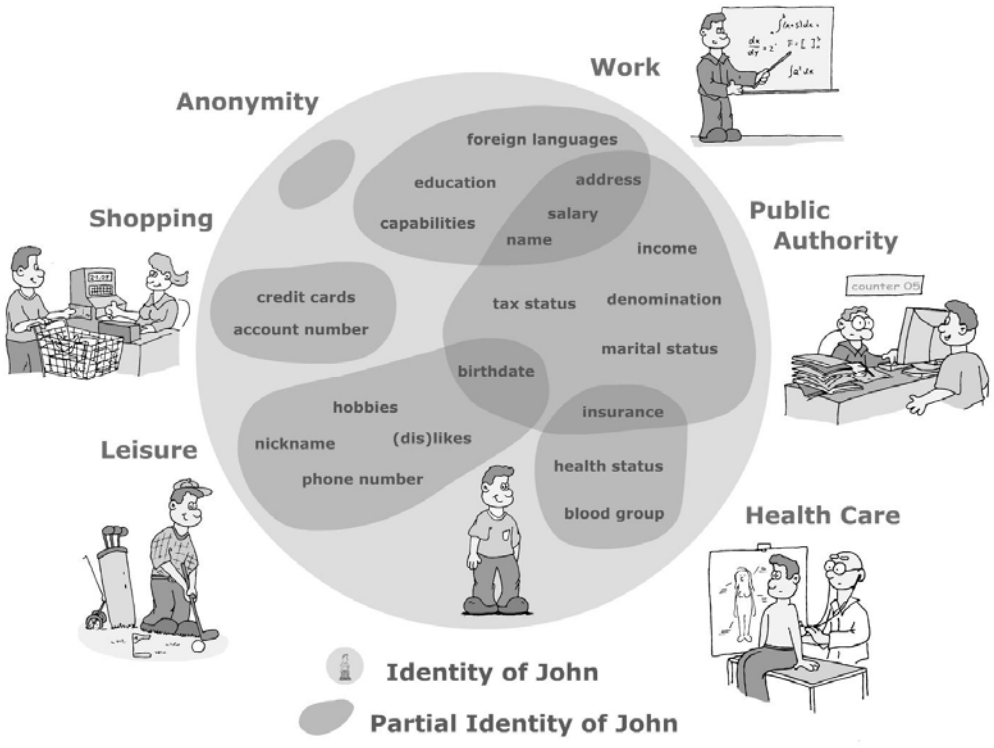


Fig. 1: John's partial identities (as shown in the PRIME tutorials (PRIME 2008))

Several relevant building blocks of privacy-enhancing identity management are briefly sketched in the following subchapters. A more detailed overview is given in the White Paper of the project "PRIME – Privacy and Identity Management for Europe" (cf. Leenes, Schallaböck, Hansen 2008) or in (Hansen 2008b). The PRIME project as well as its successor project PrimeLife aim at developing solutions for both user-controlled and privacy-enhancing identity management that supports individuals' sovereignty over their private sphere and

enterprises' privacy-compliant data processing. The guiding principle is to put individuals in control of their personal data.

3.1. Various pseudonyms and private credentials

The use of distinct pseudonyms (see Figure 2) instead of real names helps to prevent undesired context-spanning linkage and profiling by unauthorised parties. Separation of contexts can be further supported when organisations design their workflows of data processing in a proper way, e.g., by splitting up different tasks. For example, in a shopping scenario the shop could make us of separated delivery and payment services so that none of the parties involved gets to know all customer information on the bought goods, the financial account data and the delivery address.

Fig. 2: Different pseudonyms for different contexts

Even with different pseudonyms, the proof of authorisations (e.g., to be of legal age) is possible in a way that combines data minimisation and accountability. So-called "private credentials" (cf. Camenisch, Lysyanskaya 2000) or similarly "minimal disclosure credentials" (based on Brands 2000) enable proving one's authorisation without revealing information that may identify the individual. These private credentials are derived from master certificates issued on different pseudonyms of the same person. They can be created in a way that they are neither linkable to each other nor to the issuance interaction in which the master certificate was obtained. Only in the case of misuse the user's anonymity can be revoked, according to predefined conditions.

3.2. Anonymous communication infrastructure

The idea of preventing context-spanning linkage by use of different pseudonyms is only good if the linkage is not done by other means. Looking at the ISO / OSI Reference Model (see

Table 1), identifiers on all network layers can be used for linkage as well as information within the data disclosed (e.g., when telling the real name) or data in the communication environment (e.g., time or location).

Table 1: ISO / OSI Reference Model

No.	Layer	Function
7	Application Layer	Network process to application
6	Presentation Layer	Data representation and encryption
5	Session Layer	Interhost communication
4	Transport Layer	End-to-end connections and reliability
3	Network Layer	Path determination and logical addressing
2	Data Link Layer	Physical addressing (MAC (Media Access Control) & Logical Link Control (LLC))
1	Physical Layer	Media, signal and binary transmission

However, the “need to know” principle also applies to the communication infrastructure: Providers do not need to know what is communicated to whom at what time. Comparable to the legally demanded secrecy of the post, there is the required secrecy of telecommunication which should protect the content of messages as well as the circumstances on sending or receiving them.

For Internet communication, a relevant identifier is the IP address. An anonymous communication infrastructure aims at making the usage of the communication network anonymous against unauthorised entities. For IP address anonymisation, different approaches have been discussed, starting with (Chaum 1981) where even the providers of the anonymisation service cannot identify the user’s original addresses unless they put together their knowledge. With the AN.ON anonymisation service, users can use the World Wide Web while sharing one common IP address so they can surf anonymously. Their anonymity regarding the IP address is protected unless there is a judicial decision to revoke the anonymity of a specific individual (cf. Köpsell, Wendolsky, Federrath 2006).

3.3. Showing and enforcing policies on data processing

Privacy policies of web sites are well-known. They usually contain information on how the service is going to use the users’ data and who can be addressed in case of questions. Sometimes they also explain what safeguards against unauthorised access are in place.

Since the late 1990ies there had been attempts to make privacy policies machine-readable, e.g., via the Platform for Privacy Preferences (P3P): The objective is to enable the user's personal computer to show and interpret the privacy policy in an understandable, standardised way, and possibly to interact with the user in case of choices or complaints. Although by now there is no widespread adaption of this or other policy languages, it is a promising way to go: It enhances clarity on data processing for the user who may not be willing or able to understand the legalese of longish privacy policies which may even be written in a foreign language. This may also be good for Data Protection Authorities which can check the legal compliance of the policy and evaluate whether the actual data processing matches the statements in the policy. And finally the services can use technologies to help them automatically enforcing what they expressed in the privacy policy.

Similar policies could also be directly attached to all kinds of data and be stuck to them even if the data are transferred to other parties. The so-called "sticky policy" paradigm (cf. Karjoth, Schunter, Waidner 2002, Casassa Mont, Pearson, Bramhall 2003) aim at automatic enforcement of the policy statements at the data controllers. Usually this concept cannot entirely prevent unauthorised access by attackers, but at least it can make it harder and can minimize errors stemming from careless data handling.

When discussing legal compliance, rights and obligations, the national jurisdiction of data controllers concerned and the location of data processing serves as a rule. Although written data protection law is not automatically being enforced and although in the Internet there is an enforcement deficit, the legal system should not be neglected. This makes it necessary for the user to know beforehand the jurisdiction the data processing may fall in. Not only the data controllers' (and their contractors') jurisdiction is important, but also the routing of, e.g., IP packets can be relevant here.

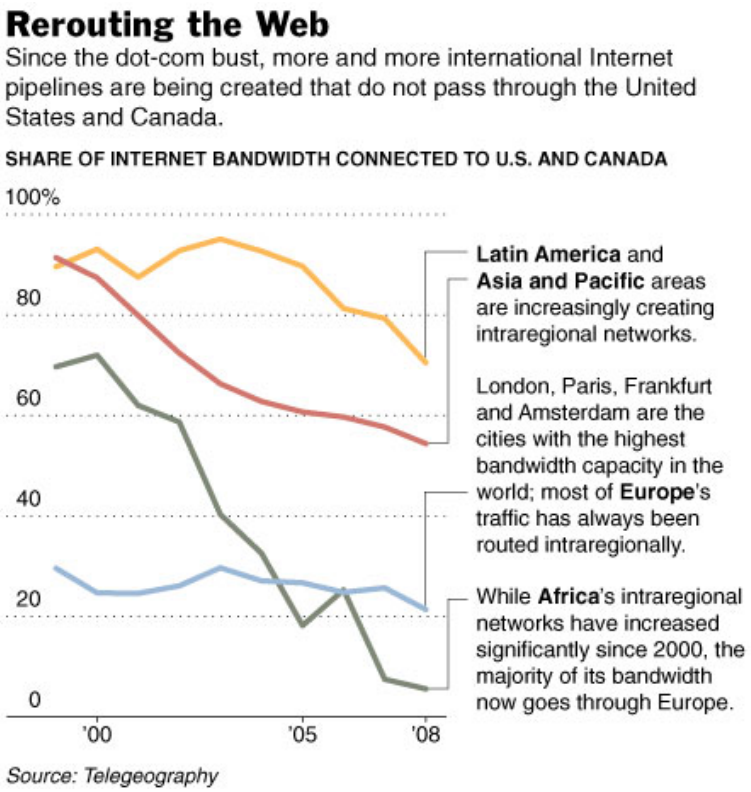


Fig. 3: Routing of IP packets via the United States (Source: Telegeography, quoted by Markoff 2008)

Still a big amount of inner-European Internet traffic is routed via the United States of America (see Figure 3) although it is decreasing – and according to a recent news posting, this "may have intelligence – and conceivably military – consequences" (Markoff 2008). This makes clear that technical processes such as routing may have a severe impact both on privacy and security, and of course also on economics if other countries can – fully in line with their own legal provisions and the tasks of their secret service – intercept transferred data meant to stay in Europe. Ways to determine the jurisdiction before data transfer begins and show that to the user are necessary if data should be kept in the realms of the European Union – be it for privacy or security reasons (cf. ENISA Ad Hoc Working Group on Privacy and Technology 2008).

3.4. Support to exercise privacy rights

According to European jurisdiction, individuals have the right to request access to their personal data, rectification of inaccurate personal data and erasure of illegally stored data. In addition they can withdraw a formerly given consent. Only few individuals are aware of their rights (cf. Eurobarometer 2008), and for those who choose to exercise them, it can be quite cumbersome, e.g., because it usually requires to write letters to data controllers.

Remedy can be produced by offering easier ways to exercise one's rights, e.g., by online access for individuals (cf. ENISA Ad Hoc Working Group on Privacy and Technology 2008) or by tools which help them to find the responsible data controllers (which sometimes is a hard problem) and to manage their correspondence with them (cf. Hansen 2008b). If necessary, the

Data Protection Authority in charge could also be informed about possible violations of the law. Similarly, contacts to consumer protection organisations could be established.

3.5. News feed on security and privacy incidents

Not in all countries, the legal obligation exists to inform people concerned about security and privacy incidents where, e.g., personal data may be accessed by unauthorised parties. But even if there is a kind of security breach notification regulation, it is not clear whether individuals really profit from that: How should they behave when they get to know that they became victims of a security breach? And how can they estimate the actual risk for the present and the future? Indeed these are important questions, but it is no alternative if organisations are allowed to suppress the information on relevant security breaches.

In PRIME's identity management research and development, a news feed on security and privacy threats or incidents has been proposed (cf. Hansen 2008b). In the identity management system at the user's side, the news items can be evaluated according to relevance to the user, e.g., which data had been disclosed to the data controller or in which contexts a tool had been used where security vulnerabilities may have been exploited. Data controllers should be encouraged to inform the persons concerned in a way that they are empowered to act, e.g., by configuring and patching their systems accordingly, by dropping the pseudonym used before, by changing account data, by requesting information from others who may have gotten access to the personal data or by bringing the case to court.

3.6. Full audit trail

In information society, data is an important asset. As far as data of a person are concerned, privacy control is only possible if observation, linkage and analysis of the data, performed by potentially different parties, can be understood or even traced. Figure 4 sketches a typical workflow of data which may lead to decisions about, e.g., receptiveness to marketing information, creditworthiness, suitability for a specific job, or probability of contracting a particular disease in the next decade (cf. Hansen, Meissner 2007, in more detail discussed in Hansen 2008a). These decisions may affect a group of people or a single individual.

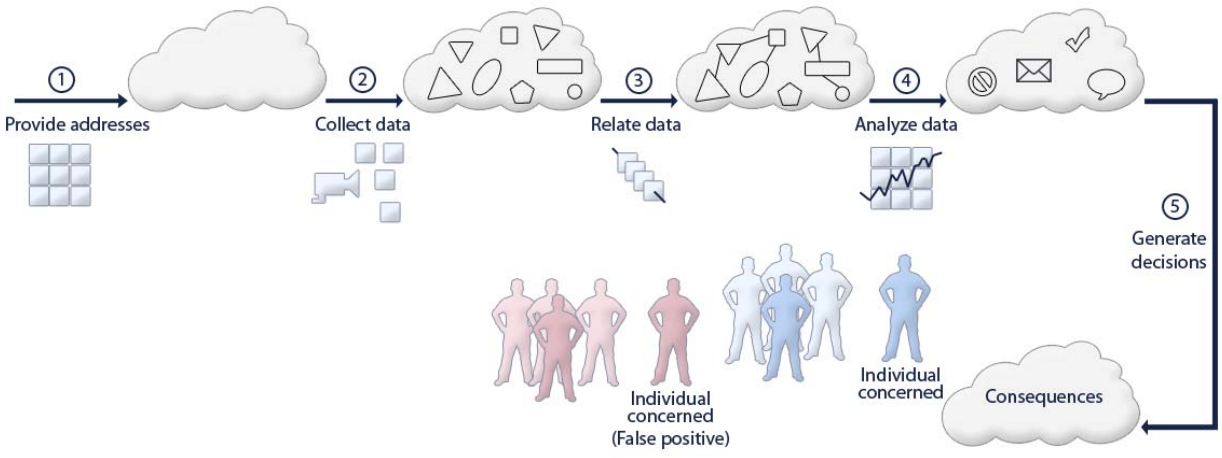


Fig. 4: Workflow of data enrichment influencing an individual's privacy

With a full audit trail for all parties dealing with the data, better transparency could be achieved about all data processing involved, about the responsible actors performing data processing, and about used algorithms and tools when enriching personal data. A process to tackle complaints, to find out how decisions had been generated and to correct and improve the data enrichment workflow would have to be added. In other areas of production, e.g., in the medical sector or when building modern planes like the Airbus, this kind of audit trail is well-known. In the data protection area, the logging obligations and methods would have to prevent the creation of additional risks to privacy by the audit trail itself.

4. Matching Privacy-Enhancing Identity Management with Security Objectives

Taking the building blocks from the previous chapter, Table 2 analyses how well they match with security objectives and how applicable they may be with respect to security technologies.

Table 2: Privacy-enhancing identity management methods transferred to security objectives

	Objective in privacy-enhancing identity management	**How to be used in security technologies**
Various pseudonyms and private credentials	Protection against unauthorised linkage	Prevent misuse, enable authorised singularised linkage
Anonymous communication infrastructure	Protection against unauthorised identification	Enable authorised singularised identification
Showing and enforcing policies	Make clear conditions for data processing and give information on jurisdiction as well as contacts for complaints or further questions	
Support to exercise privacy rights	Empower users, establish contacts to Data Protection Authorities / consumer protection organisations	Extension to “security bodies” possible: defined processes for access, better acceptance
Security and privacy feed	Inform people concerned on breaches	Use channel for security-related news and other communication to users *after* finished proceedings
Full audit trail	Auditability, transparency on data quality, possibility to find errors and correct them	

Indeed, the building blocks explained in the previous chapter can have relevance when designing security technologies, too:

- Pseudonyms and credentials help users to protect themselves. A better authentication level would also decrease the risk of identity theft; less linkabilities of data observed by other parties can counter attempts to espionage. The private credential concept

enables authorised law enforcement to establish an authorised linkage and identification of certain individuals under predefined conditions.

- A similar re-identification can be designed as part of a communication infrastructure with revocable anonymity. Mass re-identification and surveillance should be prevented here by appropriate technical means. For normal users, the anonymous communication infrastructure helps to protect themselves, their data and their communication relations.

- A clear information on what data processing is planned, in which jurisdiction it will take place and which possibilities for complaints or redress exist, should be natural in any case, also when data is processed by security technologies. This information should be accessible both by supervisory authorities and individuals concerned.

- The idea to exercise one's privacy rights cannot be directly transferred to security bodies as far as there are exceptions of current proceedings where suspects won't get all information. Still they have the right to be informed after the proceedings have ended. Currently this information is not always given, and often there are no well-defined processes to inform the former suspects if the case is not brought before court. This should be improved.

- The approach to inform people by news feeds could be extended to all information which is relevant to security of society. Also individuals could be addressed by this means, e.g., for information obligations as soon as transparency is due.

- It is necessary to know the degree of accuracy and completeness of data and their sources. The demand for auditability, assessability of data quality and the possibility to improve the findings and procedures when it comes to security is comparable to the similar needs from the privacy perspective. Also similar technical methods could be used. By the way, also transparency and checkability of law enforcement processes should be made possible whenever possible to enhance the acceptance of society.

Note that the sketched building blocks do not guarantee full privacy control for individuals. This would require the integration of all channels where data may be disclosed, including sensors in the environment or other people disclosing (correct or incorrect) data on the individual concerned. Also, the building blocks are not a comprehensive collection of privacy-enhancing functionality which can be part of security technologies. This text can only give a glimpse on the compatibility of privacy and security objectives at least in some areas, if designed in a proper way.

5. Conclusion

Security technologies have to respect the basic rights and needs of unsuspicious citizens. Otherwise this may significantly decrease acceptance of certain technologies or even compromise the citizens' trust in their own society and the governmental system they live in.

The state should try to protect its citizens against criminals, and where this is not feasible, it should help them to protect themselves. By no means the state should tolerate or even actively breed data security vulnerabilities, e.g., in personal computers used by citizens. Also any accumulation of data poses a risk to the individuals' privacy, no matter whether the state directly collects these data or other parties, e.g., providers who are legally obliged to do so for the purpose of data retention and provision of access by state authorities under specific conditions. Obviously giving citizen data to entities outside the European jurisdiction – as this is the case with passenger name records (PNR) – does not increase the trust in proper safeguarding the data against undesired access. Privacy and security of individuals must not be weakened, but strengthened.

Privacy-enhancing identity management offers a variety of approaches which to a big extent make sense in the context of security technologies, too. A main difference lies in the point in time when individuals concerned have to be informed on data processing: While the privacy perspective requires informing the individuals concerned immediately, from the security perspective it often can be necessary to refrain from informing the suspects until the end of the investigation so that in current proceedings transparency is not demanded. At a later point in time the information blackout is not relevant anymore, and for the sake of transparency people concerned have to be made aware in the aftermath. All in all, privacy-enhancing building blocks should always be considered when designing, implementing and operating security technologies.

Those who do not esteem the individuals' privacy as much as the author, should substitute the concept of "maintaining one's privacy" by "keeping trade secrets": The line of reasoning based on the individuals' needs of privacy for a functioning society works in the economic context aiming at keeping trade secrets in the own area of control, too. Both individuals' and economics' needs as well as legal and ethical principles have to be taken into account when designing security technologies and planning security-related processes.

Acknowledgements

This work was partially done within the context of the EU-funded FP6 project "PRISE – Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies" on privacy and security technologies. In addition it takes results from the EU-funded FP6 project "PRIME – Privacy and Identity Management for Europe" and its successor FP7 project PrimeLife. I am grateful for many helpful discussions with the PRISE team, in particular with my colleague Maren Raguse and my former colleague Jan Möller, but also with the project partners and the various experts attending the PRISE workshops. Further, I enjoyed the discourse with Andreas Pfitzmann from Dresden University of Technology on how to possibly balance privacy and security. And last but not least I thank Johann Čas from ITA for his patience and confidence when editing the PRISE book.

References

Brands, Stefan A. (2000) *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. The MIT Press

Camenisch, Jan / Lysyanskaya, Anna (2000) *Efficient Non-Transferable Anonymous Multi-Show Credential System With Optional Anonymity Revocation*. IBM Research Report RZ 3295 (# 93341), extended abstract in: Advances in Cryptology – Eurocrypt 2001, revised full version available at http://eprint.iacr.org/2001/019. Accessed 22 Nov 2008

Casassa Mont, Marco / Pearson, Siani / Bramhall, Pete (2003) *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services*. Trusted Systems Laboratory, HP Laboratories Bristol, HPL-2003-49. http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf. Accessed 22 Nov 2008

Chaum, David (1981) Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *CACM* 24 (2): 84-88

Chaum, David (1985) Security without Identification: Transaction Systems to Make Big Brother Obsolete. *CACM* 28 (10): 1030-1044

Clauß, Sebastian / Köhntopp, Marit (2001) Identity Management and Its Support of Multilateral Security. *Computer Networks* 37 (2): 205-219

ENISA Ad Hoc Working Group on Privacy and Technology (2008) *Technology-Induced Challenges in Privacy & Data Protection in Europe*. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf. Accessed 22 Nov 2008

Eurobarometer (2008) *Data Protection in the European Union – Citizens' Perceptions*. Analytical Report. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf. Accessed 22 Nov 2008

Hansen, Marit (2008a) Linkage Control – Integrating the Essence of Privacy Protection into Identity Management Systems. In: Cunningham, Paul / Cunningham, Miriam (eds) *Collaboration and the Knowledge Economy: Issues, Applications, Case Studies*, Proceedings of eChallenges 2008, IOS Press, Amsterdam, 1585-1592

Hansen, Marit (2008b) User-Controlled Identity Management: The Key to the Future of Privacy? In: *International Journal of Intellectual Property Management* 2 (4): 325-344

Hansen, Marit / Meissner, Sebastian (eds) (2007) *Verkettung digitaler Identitäten*. Report commissioned by the German Federal Ministry of Education and Research. https://www.datenschutzzentrum.de/projekte/verkettung/. Accessed 22 Nov 2008

Hansen, Markus / Pfitzmann, Andreas (2008) Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen. In: Roggan, Fredrik (ed) *Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008*. Berliner Wissenschafts-Verlag, Berlin, 131-154

Karjoth, Günter / Schunter, Matthias / Waidner, Michael (2002) Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data. In: *Proceedings of 2nd Workshop on Privacy Enhancing Technologies (PET 2002)*, LNCS 2482, Springer, 69-84

Köpsell, Stefan / Wendolsky, Rolf / Federrath, Hannes (2006) Revocable Anonymity. In: Müller, Günter (ed) *Proc. Emerging Trends in Information and Communication Security (ETRICS 2006)*, LNCS 3995, Springer, 206-220

Leenes, Ronald / Schallaböck, Jan / Hansen, Marit (eds) (2008) *Privacy and Identity Management for Europe – PRIME White Paper V3*. https://www.prime-project.eu/prime_products/whitepaper/. Accessed 22 Nov 2008

Markoff, John (2008) *Internet Traffic Begins to Bypass the U.S.* The New York Times, 30 August 2008

Maslow, Abraham H. (1943) A Theory of Human Motivation. *Psychological Review* 50: 370-396

Pfitzmann, Andreas / Köhntopp, Marit (2001) Striking a Balance between Cyber-Crime Prevention and Privacy. In: *The IPTS Report* 57: 9-17. http://www.jrc.es/home/report/english/articles/vol57/ICT1E576.htm. Accessed 22 Nov 2008

Pfitzmann, Birgit / Waidner, Michael / Pfitzmann, Andreas (2000) *Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity*. IBM Research Report RZ 3232 (#93278) 05/22/00, IBM Research Division, Zurich. http://www.semper.org/sirene/publ/PWP_00anoEcommerce.ps.gz. Accessed 22 Nov 2008

PRIME (2008) *PRIME Tutorials*. https://www.prime-project.eu/tutorials/. Accessed 22 Nov 2008

Privacy-enhancing Technologies at IBM

Phil Janson
STSM, IBM Academy of Technology, IBM Research, Zurich Lab
pj@zurich.ibm.com

Abstract:

For IBM, privacy-enhancing technologies are an important element in protecting the privacy of individuals. In this presentation we will survey the role of privacy-enhancing technologies at IBM. This has several aspects:

1. IBM uses privacy-enhancing technologies to protect the privacy of IBM's customers.

2. IBM builds products that incorporate privacy-enabling technologies.

3. IBM Research is working on advancing the state-of-the-art in privacy enhancing technologies.

Internal rules and regulations are the foundation of protecting the privacy of IBM's customers. They define the privacy objectives and processes that need to be followed whenever personal data is handled. In addition to this foundation, we employ various privacy-enabling technologies. One example is email cleansing that prevents unsolicited emails to customer by allowing them to globally opt-out of receiving emails. Another example are P3P privacy policies on all our websites.

IBM provides several products incorporating privacy-enabling technologies. One example is IBM Anonymous Resolution[1] that allows organizations to compare data (e.g., buyers against a fraud blacklist) without exchanging personal data. Another example is the Watchfire web-site and application scanning products that can identify potential privacy problems on large web-sites.

IBM participates in the open-source identity management framework project Higgins and various standardization bodies (e.g, ITU, OASIS) to support broad adoptions and openness of privacy-enhancing technologies.

IBM Research finally advances the state of privacy-enabling technologies. Research projects include IdentityMixer that allows individuals to prove attributes (such as age or membership) without revealing any identifying information. Another example is IBM's clipped RFID tags that allow consumers to remove the antenna of RFID tags in order to prevent tracing after an item has been purchased. A final project is IBM's smart surveillance that allows video recording while using image processing in the camera to automatically remove faces and other identifying information.

[1] http://www-306.ibm.com/software/data/ips/products/masterdata/eas/

IBM Research is furthermore leading the EU-funded project PRIME (Privacy-Enhancing Identity for Europe) that ends this summer and also the successor project PrimeLife which starts March 1st.

The RFID chip designed to meet known privacy and security issues

Henrik Granau
RFIDsec
henrik.granau@rfidsec.com

Abstract:

In 2004 a complete new approach to RFID Privacy and Security was published under the lead of Stephan Engberg, who is a privacy expert. A scientific Paper was issued and peer reviewed in October 2004.

In 2005 RFIDsec was founded to implement the technology and to bring secure, privacy enhanced RFID products to market.

Now in 2008, RFIDsec is delivering the products to the first Pilot Customers.

RFIDsec is offering complete end-to-end security in RFID solutions using a new secure protocol based upon the Zero-knowledge principles.

When using RFIDsec RFID tags, it is possible to make a complete transfer of control to the new owner of the tag (incl. a consumer) and the tag can be switched into 'Silent Mode', where unauthorised readers can't even detect that there is a RFID tag within reading distance.

The technology ensures;

- ✓ The RFID tags can not be identified by unauthorised reading attempts
- ✓ The RFID tags can not be cloned
- ✓ Data on the RFID tags can be protected from unauthorised access and this can be differentiated for separate areas of the memory and by Read/Write/Create access
- ✓ The communication between reader and tag can not be eavesdropped, hence protection against 'replay attacks'

The concept is that the end-user of the RFID technology is in complete control and is ensured that no information is leaked when using the RFID technology.

The RFIDsec technology has made it possible for a partner to offer RFID based solutions for transportation of hazardous goods, including explosives. With standard RFID technology this would not have been possible due to the huge exposure to crime and terror.

As the RFIDsec technology provides the possibility to perform an authenticity check, ie. ensuring the RFID tag is not a clone, the Police is able to use the RFID technology to identify lost and stolen assets, like Danish Design Furniture.

Using the RFIDsec tags on products is meeting the most obvious Privacy issues like the RFID tags leaking personal related information, turning the RFID tags into tracking devices etc., but in the areas of using RFID technology to strong identification of a person, ie. payment, passport etc. not even the RFIDsec technology is secure enough. It has to be combined with other technologies, such as various biometric technologies, ie. you could use the biometrics to open up for a secure RFID communication.

By looking at RFID tags as just barcode replacement, and especially if your focus is only on Supply Chain Management, it's difficult to understand the magnitude of the Privacy and even the Security issues.

As an attempt to make the RFID Industry aware of the importance of these issues, RFIDsec released an article 'Design patterns and Business Models for a New Generation of RFID Solutions' November 2007, where the mindset of viewing the RFID tag as a computer is introduced.

By viewing the RFID tag as a computer, all the security issues are getting obvious; you wouldn't leave a PC with important data unprotected for anyone to access in a public space.

Once you can ensure the data integrity on the RFID tag, you can start using RFID on parts of an aeroplane to increase flight safety without getting exposed to anti-counterfeiters or terrorists.

By attaching the RFID tag to an asset, you turn the asset into an intelligent asset, which will be able to communicate with you as well as other assets, hence a next step towards the Internet of Things.

RFIDsec is not claiming to be providing the only way you can solve the RFID Privacy and Security issues, but in stead of just talking about 'PETs', RFIDsec is providing actual 'PET' products.

The privacy vs security dilemma in a risk society

Vincenzo Pavone (IPP-CSIC);
Manuel Pereira (University of A Coruña)
vincenzo.pavone@cchs.csic.es

Insights from the PRISE project on the public perception of new security technologies in Spain

Abstract

Current globalization processes seem to be increasingly characterized by the emergence of equally global risks, which are now coming to the fore in all their threatening potentiality. In a way, we live in a society that Ulrich Beck has defined "risk society", in which risks no longer affect merely individuals as such but societies as a whole. These new risks materialize as a result of the combination between objective factors, such as the trans-national nature of agents and tools involved, and subjective factors, which relate to the social construction of certain events as risky and the changing public understanding of security. Whilst the interaction between these subjective and objective factors urges national and regional governments to implement new security policies and technologies, the public perception of these new policies and technologies emerges as a sort of universal measure to guide governmental actions. Current research on public perception of security technologies especially focuses on the dilemma between privacy and security. Exploring public engagement with future scenarios evoked by the implementation of new security and privacy technologies, the PRISE project analyzes the mutually constitutive relationship between the implementation of new security technologies and social construction of risk. Combining quantitative and qualitative techniques, this study, which is one of the PRISE Project's case studies, offers intriguing insights on the security and privacy discourse in Spain. In spite of the 11/3 terrorist attack and the media and governmental emphasis, it seems that terrorism is far from being the main security concern. In fact, Spanish citizens seem to be not only aware of the implications of new security measures in terms of political use and control but also afraid of the risk of commercial exploitation. Actually, they seem to hold a different perspective, which emphasizes the quality of security measures rather than their quantity. In a context of rising security concerns, expanding definitions of risk and growing governmental monitoring activities, this paper may cast some light on the persisting gap between the governmental and the lay public perception of security agenda as well as on the political implications of the new public discourse on security.

1. Introduction

The tragedy of 9/11 and subsequent terror attacks have considerably increased the political importance of security and led to the development of new security concepts and strategies that shift the balance between security and the observance of human rights. We have seen the development and implementation of new security technologies and measures throughout Europe, which are supposed to raise security for European citizens, but are at the same time increasing the surveillance of citizens and causing infringements of privacy.

As a result, the growing interest placed on security issues raised an important political debate focusing on the relationship between security and privacy as well as on the role that modern technologies may play therein. On the one hand, security and privacy have been mainly framed as a trade off, on the basis on the assumption that any increase in security levels would inevitably curbs the amount of privacy enjoyed by any single citizen. On the other hand, the rapid uptake of new security technologies, which has allegedly occurred at the expenses of democratic scrutiny and social participation, urged the debate to focus either on the potential technocratic implications or on the possibility of authoritarian slippery slopes.

Either way, the debate on "securitisation" (Waever, 1995) has indirectly contributed to cast some light on some of the several implications of the risk society thesis, advanced by Beck in 1992. Approaching the issue of globalization at the very end of the Cold War, Ulrich Beck pointed out how current globalization processes seemed to be increasingly characterized by the emergence of equally global risks, which were expected to come to the fore in all their threatening potentiality very soon. In Beck's opinion, western societies were essentially characterised by the common sharing of new and inherently trans-national risks, which could no longer be isolated and approached from a national point of view but needed to be studied and understood from a global perspective. Insisting on their permanent rather than transitory nature, Beck came to the conclusion that these risks were transforming western society, as it moved with increasing speed into the process of globalization, into what he defined a "global risk society".

Drawing on Beck's ideas on risk society, we will now try to make a contribution to the general debate of *securitisation* emerged around the privacy and security dilemma and the political implications raised by security technologies, by looking at the citizens' perceptions of new security and privacy technologies in Spain. In the first two sections, we will explore some of the relevant literature on the issues of security, risk and technologies, paying attention to both the theoretical framework inspired by the risk society thesis and to the most recent debate on technology, security and democracy. In the central section, after having introduced our research questions and hypotheses, we will then outline the methodology employed and present the main findings of the interview meetings. In the conclusion, we will reconsider the literature on the privacy and security dilemma as well as the framework provided by the risk society in the light of these findings.

In fact, the findings of the interview meetings have produced unexpected outcomes, which not only show that the public is not willing to uncritically renounce to their privacy in exchange for more security but also that the public is aware of the eminently political role played by the spreading discourse on terrorism and security. In a context of rising security concerns, expanding definitions of risk and growing governmental monitoring activities, this paper may cast some light on the persisting gap between the governmental and the lay public perception

of security agenda as well as on the political implications of the new public discourse on security.

2. Living in a risk society

In 1992, Ulrich Beck published a work in which he reconsidered the process of modernity and tried to outlined its recent developments and contradictions, suggesting the materialization of a new form of modernity, characterised by the emergence of a "risk society" (Beck 1992). The publication of the Risk Society thesis was then followed by a growing debate, in which contributions and criticisms blossomed to the extent that the risk society approach has been used in fields as far apart as security and medicine. After September 9/11, Beck re-assessed its original approach and made a few contributions to the ongoing debate, clarifying his ideas on the terrorist threat (Beck, 2002) and re-proposing his "second modernity" as a research agenda (Beck, Bonss and Lau 2003; Beck and Lau, 2005). In Beck's view, it was necessary to move beyond the usual counter position between traditional and modern societies, as the latter was about to enter into contradiction with its own premises and principles (Beck, Bonss and Lau 2003:6). In fact, Beck suggested that the western society had entered a new phase of its own history, which he named "self-reflexive modernity", in contrast to the traditional modernity emerged as a result of the Enlightenment. Given that western societies were and remains essentially modern societies, self-reflexive modernity, however, should not be considered as a "post-modernity" as no radical break with traditional institutions of modern societies seems to have occurred (Beck 2005: 526).

In fact, these institutions are rather experiencing a process of transformation resulting from a *radicalization* of the modernization process, which has produced a gulf between the world of quantifiable risks in which we were used to act and the world of non-quantifiable global risks associated with environmental changes, financial markets and terrorist threats that this process of transformation is creating (Beck 2002, 40-44). As a result, modern institutions – like the nation state, the welfare system and the nuclear family – and basic modern principles – such as the very idea of control and security, the binomial connection between science and rationality and the exploitation of nature as recipient of external resources – are increasingly questioned by the expansion of globalization and the intensification of individualization. The latter are forcing modernity into a reflexive state, which Beck, quoting Latour, defined as a situation in which "there is a heightened awareness that mastery is impossible".

In these recent articles, Beck, Bonss and Lau have extensively outlined the variety of fields and institutions that the transition to self-reflexive modernity is affecting. Whilst globalization is producing a vanishing of borders and the re-evaluation of the role and limits of the nation-state, the radicalized process of individualization is not only challenging the very foundations of the welfare state system but also producing an erosion of the several patterns of collective life. At the same time, the gradual acknowledgement of the scarcity of basic natural resources and of the devastating impact of pollution and human exploitation has generated the perception of a global ecological crisis, which is shaping a new understanding of nature as part and parcel of society. These fields and institutions are permanently being redefined and restructured in a context where traditional distinctions, like we/others, nature/society, global/local, war/peace or public/private, experience a permanent process of blurring boundaries (Beck, Bonss and Lau 2003: 18).

These transformations, Beck specified, are not due to exogenous factors but to the radicalization of the driving forces structurally belonging to the first modernity, which seems to have produced largely unintended side-effects that began to be visible only in recent times. These side-effects derive from the modern system of production of goods and wealth, whose radicalization, structurally associated with the production of risk, is ultimately leading to the instauration of a risk society, in which risks no longer affect merely individuals as such but societies as a whole (Beck 1992). In a risk society, to put it in Lash's words: "individuals must live, are forced to live in an atmosphere of risk in which knowledge and life chances are precarious." (Lash 2001: x).

It is important to clarify the distinction between risks and dangers. Niklas Luhmann, for instance, suggested that risks emerge as a consequence of human action whilst dangers arise from natural phenomena proceeding from the external world (Luhmann 1993). Whilst in the first case, human beings can, and usually do, evaluate, balance and act in response to their risk assessment, in the second case human beings are often merely in position of minimizing the adverse consequences of the materialization of a danger. Beck adopts a similar approach, defining dangers as belonging to nature and risks as belonging to the realm of human action and decision making. In the second modernity, however, risks are no longer calculable and predictable, as the modern narrative held them to be. Global risks are uncontrollable (Beck 2002: 40).

Human societies of all times had to face risks of various sorts, from poverty to war, from pandemic diseases to internal rebellions, but the risk society deals with risks that present somewhat different characteristics, as they often do not appear in the same space or time in which they had been originally emerged (Beck, 2006:33). In several cases, these risks are not observable by the citizens, as they proceed from technological devices, environmental changes, financial exchanges or security threats that are cannot be immediately identified or observed. In a risk society, citizens are made aware of these risks through the experts, the media or the political debate (Beck, 2006: 35).

Among all the risks generated by the transition from first to second modernity, Beck paid special attention to the dynamics of risks and risk perception triggered by the global terrorist threat following the 9/11 attack. This event produced a twofold reaction, which set in motion new narratives and practices related to security and democracy. On the one hand, it materialized a global threat, external to western society in philosophical terms but internal in structural, social and political terms. In other words, the enemy was clearly identified in abstract terms as "alien" to western culture but physically placed everywhere, within national borders, among all citizens, in a potentially unlimited setting that defies spatial and temporal localization (Beck 2002:44). This new definition of the terrorist threat, which redefines traditional boundaries between inside/outside, us/others, has in turn set in motion a redefinition of security, politics and democracy.

On the one hand, in a world risk society confronted with a universal terrorist threat, suddenly government matter again and the state is back to serve the most traditional of its functions, i.e., the provision of security. On the other hand, the nations of western world united against the common threat, making it necessary to redraw the geopolitical map of the world, producing a close interlocking of national security and foreign policy. Finally, the walls between innocents and guilty collapsed, extending suspicion to all citizens, without exception: "under conditions of a universalized perception of terrorist threats all individuals are potentially suspects and all

individual rights constitute potential risks to the state" (Beck, Bonss and Lau 2003: 12). Vulnerability and fear are, thus, normalized, ceasing to be problematised (Spence 2005).

This specific aspect of a global risk society carries several significant political implications. First, privacy and security came to be framed as opposing each other in a trade-off whose balance has to be permanently negotiated. Second, the state has re-affirmed its role of security provider *at the expenses* of another traditional role, the institutional setting preserving and enabling democracy and individual rights. Third, the solution has been often sought at the technological level, producing a new narrative of security that remarkably confirms the overlapping of first and second modernity currently shaping western politics.

On the one hand, the global and unpredictable nature of terrorist threats is acknowledged whilst, on the other hand, the solution is offered following the modern scheme, which, following the rationality principle, usually seeks to control and dominates problems through the implementation of new technological devices within the territorial boundaries of the nation state (Beck and Lau 2005; Duffield and Waddell, 2006). Based on a doctrine of absolute security that does not allow realistic strategies of risk reductions, these technological and territorial responses to the risks generated by global terrorism, such as pre-emption, surveillance, border controls and pervasive monitoring, have marginalised any attempt to reasonable negotiation of risks, contributing to an intensification of terror (Spence 2005).

Under this new frame, which shares with first modernity the basic principles but elaborates new institutions according to the second modernity challenges (Beck and Lau 2005, 533) privacy and security are constructed as a zero-sum game whilst governments seeks technological solutions to political problems (Levi and Wall 2004, 201). However, in accordance with the cognitive revolution in which western society enters as it advances towards reflexive modernity, the solutions provided by the introduction of new technology are increasingly perceived as socially problematic and scientifically uncertain. In turn, public participation in participatory technology assessment is introduced as part of a new endeavour that tries to use both scientific and non-scientific knowledge as reliable bases for decision making.

In fact, the rapid progress in the development of communication technologies, biometrics, sensor technologies and data storage and analysis capabilities are perceived as causing constant pressure on the fundamental right to privacy for both economic and security reasons. The final outcome is a pragmatically oriented policy making that introduces new technologies to enhance security whilst it embodies participatory technology assessment exercises in order to preserve public trust, restore political legitimacy and enhance democratic accountability.

In the following section, we will first explore how security, terrorism and democracy may be fruitfully addressed within a risk society perspective and then we will revise some of the most relevant literature on security technology and privacy. Finally, we will outline the research questions and move into the fourth section, in which the findings of the PRISE project will be presented.

3. Security, technology and democracy in a risk society

One of the main issues addressed by the risk society approach is the overlapping between first and second modernity principles and institutions. This seems to be especially true in relation to the most recent developments in security and technology policy. The latter's emphasis on technological responses to socially constructed security needs emerges as especially problematic because scientific knowledge is experiencing an important redefinition, as it is no longer perceived as an objective basis for political decision making. The growing exposure of scientific dissent within the scientific community, usually paralleled by the manifestation of emerging conflicts among different groups of scientists belonging to distinct scientific fields brought to the fore not only the existence of multiple rationalities but also the blurring boundaries between scientific and unscientific, scientific and politics. This process has advanced to the point that, first, sciences have no longer the power to end disputes and, second, that scientific disputes got increasingly intertwined to social and political debates, usually inspired by the parallel involvement of philosophy and sociology of science. The main issue, here, is that in the field of policy-making, decisions need to be taken even if the 'multiplicity of scientific alternatives' has been acknowledged.

As a result, policy making debates increasingly reach policy decisions without relying only on the authority of scientific knowledge. In fact, the "*choice between alternate methods of solutions does not flow of itself from scientific method. Instead it is generally derived from a variety of extra-scientific criteria*" (Beck, Bonss and Lau, 2003:16-18). Actually, policy debates have opened up to non-scientific knowledge paving the way to public perception of technology studies and to the introduction of participatory technology assessments, mainly to address what is perceived as a crisis of both cognitive and democratic legitimation (Beck 2003: 14-15). The role of public opinion and participation, therefore, becomes crucial in all the social and political domains in which new technologies are going to be implemented and security is no exception to the rule.

In fact, security is one of the fields in which the emergence of new risks has produced dramatically rapid policy responses, both at national and international levels. These news risks, in fact, materialize as a result of the combination between objective factors, such as the trans-national nature of agents and tools involved, and subjective factors, which relate to the social construction of certain events as risky and to the changing public understanding of security. As a consequence, whilst the interaction between these subjective and objective factors urges national and regional governments to implement new security policies and technologies, the public perception of these new policies and technologies emerges as a sort of universal measure to guide governmental actions.

This is especially interesting because one of the main implications of new terrorist threats is that they seems to be replacing *active trust*, which is a prerequisite of democracy as well as in the fields of economics, with a*ctive mistrust* (Beck 2003). Whilst this may potentially undermines the solidity of collective political patterns at national level, it is also questioning the validity of the *homo œconomicus* as a model for social and political interactions. As outlined by Ekberg, new communities are emerging, united by an increasing vulnerability to risk, in which the fundamental socio-political values of liberty, justice, equality and democracy are at risk (Ekberg 2007). As Beck put it, "in the terrorist society the world of individual risk is being challenged by a world of systemic risk" (Beck 2002, 44). Under conditions of systemic risk, the dominant questions relate to a) how to negotiate and distribute the costs of terrorist threats and b) who defines the identity of trans-national terrorists. In turn, this seems to have

induced policy makers to adopt a pre-emptive approach that prioritises anticipatory proactive stances to avert probabilistic scenarios (Heng 2006). Global systemic risks are set, and defined by governments and then presented to the public through the media. In fact, governments claim to be the only actors entitled to decide who, when, where and to what extent there is a terrorist threat, who are these terrorists and how the state and the citizens are supposed to deal with the menacing enemies.

Under these conditions, the relatively dominant position enjoyed by the government and the media in constructing and promoting current narratives of global risks, therefore, becomes a key question, which is likely to shape the course of present and future international politics. In the US, for instance, the governmental definition of the nature of terrorist threats, massively spread by the media, has produced a dynamics in which Bush's governmental authority and the potential power of the terrorist organizations mutually reinforce each other. In turn, this has encouraged the emergence of a narrative where permanent mobilization of the citizens is required, military budgets needs to be increased and civil liberties need to be restricted (Beck 2002, 45). In fact, as Spence pointed out, the mutual reinforcement between war on terror and terror itself is endorsing a new form of economic context, which he defined *economics of fear*, in which citizens are encouraged to a) politically mobilize in the name of homeland security whilst, at the same time, b) consume for the benefits of the national economy.

Not surprisingly, some authors recently began to focus on the impact of technologies on international relations. Charles Weiss, for instance, argued not only that many of the new events and phenomena on contemporary world politics have been made possible by new technologies, from nuclear weapons to IT technologies, but also that new technologies are likely to play a crucial role in the future developments of global governance. As a consequence, he convincingly suggested overcoming the isolation of science and technology from the 'mainstream' of international relations (Weiss, 2005). In the same vein, Erikson and Giacomello claim that security studies have not yet paid serious attention to information technology related security issues (Erikson and Giacomello 2006). The issue of technology, security and privacy in the European society after 9/11 has been extensively discussed by Levi and Wall in 2004. Whilst it is clear that after 9/11 several new 'soft' and 'hard' security measures have been introduced in Europe, Levi and Wall demonstrate that the re-securitisation of society and politics had began before the Twin Towers collapsed and that these new technologies were introduced to integrate already existing security measures, within the boundaries of an already existing legal framework. Although it is true that these events paved the way to those proposals that previously would not have been found politically acceptable, the implementation of new security technologies is currently facing two major challenges. First, they are gathering poor quality data that are difficult to integrate and produce little improvement in terms of the reduction of crime risks. Second, they are *de facto* encouraging new forms of crimes that settle outside the monitored reality, such as identity theft, illegal navigation through the flaws of software systems and underground economic and financial transactions (Levi and Wall 2004).

Addressing the issue of security technology and its potential authoritarian implications, Angela Liberatore, on the one hand, acknowledges the growing implementation of security technologies in the EU, but, on the other hand, she argues that this new emphasis on security and technology is accompanied by significant attempts at further democratising the EU, through the growing role played by public participation and scrutiny. In the end, she argues that the existence of a plurality of actors involved in the policy making processes on security enhancement provides a relatively safety net against totalitarian outcomes, whilst, at the same

time, ensuring the gradual emergence of the EU as a new security actor and as a supranational democratic polity (Liberatore 2007). Whilst Shearing (2005) wonders whether the new emphasis on risk-focused technologies is triggering the emergence of a new form of justice, less centred on individual punishment, Elia Zureik explored the social, political and economic dynamics leading western governments to promote biometrics and surveillance technologies. In her work, it comes to the fore how the political exploitation of public fear, the lobbying effort of the industry and the tight connection between economic and political interests made technology uptake a crucial factor of security policies across the globe (Zureik 2004).

Debate has taken place also around the definition of security. Whilst during the 1990s security had increasingly focused on *human* security, emphasising the role of integrated, global system of international intervention to complement the effort of ineffective states in securing their citizens, the war on terrorism seem to have encouraged an explicit re-evaluation of *homeland* security into the new global context (Duffield and Waddell, 2006).

Finally, as previously mentioned, current research on public perception of security technologies has especially focused on the dilemma between privacy and security (Bowyer 2004; Strickland and Hunt 2005). Some authors suggested that face recognition technology, and security technologies in general, are likely to force us to renounce to some of our liberties to enhance security. Provided that security technologies are effective in delivering the benefits claimed, which is controversial (Jain, Ross and Uludag 2005), they are likely to force us to make a clear distinction between those liberties that are inessential and can be sacrificed to security needs and those that are, indeed, essential and cannot be included in the trade-off (Bowyer 2004). An empirical study on RFID technology has recently focused how people understand the impact of RFID technology and whether it consciously consents. The study, based on a survey, came to the conclusion that there is a generalised lack of understanding, usually accompanied by a sense of mistrust, which calls for governmental regulation (Strickland and Hunt 2005).

Drawing on the theoretical framework of a risk society, and inspired by its most intriguing questions on the relationship between risk, technology and politics in the transition from the first to the second modernity, this study aims at exploring in deeper empirical details the relationship between security, technology and democracy as it is perceived and framed by Spanish citizens. Combining quantitative and qualitative methods, our work tries to address the following research questions. First, how do citizens actually frame the implications of security technologies? Second, do they frame security as a negative function of privacy and, if so, to what extent are willing to surrender privacy and liberty in exchange for more security unconditionally? Has terrorism made the public highly sensitive to the issue of security and, if so, what are the security threats they perceive as most urgent and compelling? And finally, are they aware of the potential political implications of framing liberty as a function of security?

In the following section, we will present the main findings of the study as well as its methodology. Finally, we will reconsider these findings in the light of the previous discussion on the dilemma between privacy and security and on the political implications of security technologies.

4. Exploring security and privacy in Spain

Exploring public engagement with future scenarios evoked by the implementation of new security and privacy technologies, the PRISE project analyzes the mutually constitutive relationship between the implementation of new security technologies and social construction of risk. Combining quantitative and qualitative techniques, this study, which is one of the PRISE Project's case studies, offers intriguing insights on the security and privacy discourse in Spain.

To explore the public perception of security technologies, and to analyze public understanding of the democratic issues at stakes, as well as the ways in which the dilemma between privacy and security comes to be framed, we have employed a methodology named “interview meeting”. At an interview meeting a group of 25-35 citizens are asked about their perceptions and preferences in relation to the implementation of a new technology. As a rule, interviewees do not possess any expert or professional knowledge about the technology in question. However, prior to and during the meeting, the participants are informed of the advantages and disadvantages of the technology in order to give them a common starting point, as balanced and factual as possible. In the PRISE project, this information is based on the scenarios developed in WP4 and the dilemmas these scenarios focus on. The purpose of the scenarios is to make it possible for participants to imagine the consequences of introducing new security technologies into the society.

As a rule, the interview meeting tries to include and explore diverging opinions and the variety of opinions among citizens. Consequently, it includes a diverse selection of citizens, selected on the basis of demographic criteria such as age, gender, education and occupation The purpose of the interview meeting, however, is not to give a representative answer on citizens’ opinions but to give an indication of what the majority of diverse group of citizens think and feel about a certain technology and, more important, give a picture of the diverse opinions and the arguments behind them.

The interview meeting is based on a combination of two methods: a small-scale survey and a focus group interview. By combining these two methods it is possible to get both qualitative data on the citizens’ opinions and small-scale quantification of these data. In the survey citizens are asked a number of questions in a written questionnaire. Subsequently the answers of the questions can be summarized in percentages and tables. This gives a picture of what the whole group of participants thinks and feels about security technologies and privacy and of the variations in the group. In this paper, however, we are very careful not to generalize the results of the interview meeting, as the number of selected citizens is not representative for the population as whole.

The combination between survey and focus groups is necessary because the survey alone may turn out to be a narrow method when dealing with complex issues. Complicated questions are often too open for interpretation by the interviewee or too hard to understand. A questionnaire gives no indication about the reasoning behind the answers, thereby excluding a crucial part of what we look for. Finally, a survey only gives a ‘snapshot picture’ of the present and does not indicate how public opinion changes through deliberation. The focus group interviews counterbalance the limitations of the survey. From the focus groups new and unpredicted knowledge is added to the analysis when the participants speak their mind, reveal their reasons and approach the subject in their own ‘language’. The discussions also give the participants a possibility to find a common ground and to develop consensus.

Although this method was common to all countries in which the PRISE project has been implemented, in Spain we have arranged four separate meetings rather than one joint event due to Spanish working hours and after work habits. Considering that mailed invitations would be regarded as 'spam', we also followed a different recruiting process based on advertisements and targeted diffusion of recruitment forms, which proved more conducive to the needed feedback.

Spain promised to be a very interesting case study, for two main reasons. First, the advancement of technology plays an important role in contemporary Spanish society, not only for its economic impact but also for its social implications and repercussions. As demonstrated by several enquiries conducted by the FECYT (1996, 2001, 2006) and by the Eurobarometer (2006) on the public perception of science and technology, the Spanish society seems to hold a benevolent and supportive attitude towards the development and application of new technologies. This study actually confirmed how this attitude also includes security and privacy technologies, as they are expected to improve citizens' security and the general protection of properties and goods. The level of support towards new security technologies, however, varies along with the perceived negative impact on citizen's privacy, in a sense that is higher when the perceived impact on privacy is lower. Such positive attitude towards the new technologies has been also extended to the very process of technology assessment hereby carried out, which has been considered a good example of the participatory processes that should always be carried out in relation to the development and implementation of new security technologies.

The second reason relates to the specific context of Madrid. Madrid is Spain's capital, a city with a large population that not only is accustomed to security technologies and extensive surveillance, but it has also been directly affected by the terrorist threats both in the past due to ETA actions and recently, in March 2004, when Al Qaeda members made several bombs explode in a number of trains converging to the central station of Atocha. Actually, the interview meeting took place a few days after the ETA had declared the end of the cease of fire, announcing a return to terrorist activity.

Surprisingly, however, in spite of the huge emotional impact of the11/3 attack and the media and governmental emphasis on terrorism, the latter seems to be far from being the main security concern among the participants. In fact, the participants not only were aware of some of the social and political implications associated with the introduction of new security technologies but they also seemed to emphasize the quality of security measures rather than their quantity.

The majority of the participants, in principle, acknowledged the need to introduce new security technologies, although usually showing some concern for the risk of privacy infringement. However, some participants clearly stated that if we have nothing to hide there is no problem in being monitored; whilst others argued that if we have nothing to hide there is no reason to be monitored.

> *These things are necessary; they help us to move on with transparency, if you have nothing to hide… I think it is necessary...*
>
> *If I have nothing to hide, why should they monitor me?*

The general concern for privacy infringement, thus, gave raise to two different reactions among the participants. In the first case, the participants felt that the privacy margins are increasingly smaller, and suggested that the new security measures may be used for perverse and illegitimate purposes. In their opinion, the increasing implementation of new security technologies is not justified by real dangers but by a growing diffusion of fear among the citizens that is purposively encouraged by the government in order to set up a more effective form of control and manipulation.

Within this framework, these technologies were not expected to really enhance the feeling of security but, confirming the hypothesis advanced by Spence, to produce the opposite result, i.e. an increase of the sense of fear and vulnerability. These technologies, thus, were perceived as pervasive and, often, ineffective in relation to their official purposes. In this view, we are all vulnerable in a way or another as there is a risk we may soon live under a 'police state' in which we all monitor each other. The general feeling proceeding from these types of comments was one of anxiety, fear and vulnerability.

In the second case, the participants generally accepted the need of introducing new security measures to contrast what they perceive as real risks, proceeding from different sources: terrorism, organized crime as well as common criminality. This group of people, in the name of security, would some of the inconveniences that may derive from the implementation of these technologies. In general, they did not feel that their privacy was affected in a serious way because they believe they have nothing to hide and because they believe that there is nobody really interested in monitoring ordinary people's life. Even if this was the case, they suggested that a massive monitoring would not be viable on practical grounds, anyway.

As a consequence, the concern about privacy's infringement is more evident among those who believe that the use of these technologies is vulnerable to be manipulated and diverted to other purposes. In contrast, the people who believe that this possibility is not going to affect them directly because they 'have nothing to hide' show a much lower level of concern. However, both types of participants came to an agreement in relation to some specific issues. First, they all agreed that 1) individual privacy should never be violated unless there is a specific and probable criminal act to investigate or prevent and that 2) being monitored is always unpleasant, especially for ordinary citizens who have no criminal intention.

The debate among the participants often focused on the concept of 'fear', giving again raise to two main positions. Whilst some participants emphasized the need of improving security, as a consequence of a sense of fear arising from risks that were perceived as real, others argued that this sense of fear is exaggerated and purposively induced among the citizens by a variety of 'interests' that would benefit from a higher level of fear among the population. It is this exaggerated and, in a way, artificial sense of fear that is needed to ensure the acceptability of new security measures and technologies.

> *"Most of the times, they sell us security, for the benefit of the economy… depending on their interests they sell us security. I have never been so monitored before 9/11".*

> *"If they didn't scare us, we would never accept, if there hadn't been a terrorist attack we would never pass through a scanner eight times in a row".*

To many, this concept of 'artificial fear' was the key to an ongoing process based on a growing disinformation that was described as aiming at the manipulation of reality. By the same token, some individuals argued that social reality was ultimately inaccessible and that, therefore, it was very difficult for ordinary citizens to discern what was real. As they argued, this situation made them more vulnerable to being manipulated in many different ways; within this framework, the media are meant to play a crucial role. "*The media are talking about terrorism every day, I usually watch the TV debates every morning and it is amazing…"*. Either way, the proponents of both positions described the 11th of September as a triggering factor behind the evolution of this process.

Whenever possible, the general solution to the trade-off between privacy and security was formulated in terms of individual choice, leaving individuals free to choose whether to use the new technologies or not. This gave raise to a contradiction, which was acknowledged by the participants themselves, among individual choice and the overall effectiveness possibly deriving from the general introduction of the new technologies.

Discussing the actual application of the new security technologies in relation to real cases, the large majority came to the conclusion that these technologies may well reduce the risks but will never be able to eliminate them. Apart from a general assessment in terms of privacy's infringement, the participants often questioned the validity of these technologies in terms of real effectiveness, showing a general attitude of mistrust, which was common to otherwise very different opinions. This attitude of mistrust seems to confirm the transition from active trust to active mistrust outlined by Beck. More specifically, the participants expressed serious doubts that the technologies could really exercise a strong preventive power in several of the scenarios proposed, although they acknowledged some dissuasive power. First, the new technologies will never be able to cover it all: "there will always be holes" and, second, the criminals are capable of fooling the security systems. I quote:

> "*I believe that catching a plane does not carry the same risk of shopping in a shopping mall, that is, they can always put a bomb in a plane as well as in any other place, and you can't monitor all of them*"

> *"Well, I believe that no matter how many cameras, how much security you have, I believe that the terrorists are actually kind with us ... they can always fool all these technologies"*.

Third, the real effectiveness of these technologies depends on the capability of the individuals actually dealing with the acquired information. In this respect, the participants used 'capability' to express both the technical/professional capability as well as the moral/ethical one.

> *"I don't know, how many of these CCTV cameras are attended by security guards, which is a job like many others, I mean it does not entail special requirements. I mean, if you spend your time monitoring people and you have to decide whether any person is showing a 'strange' behavior, you really need to have some knowledge about people's attitudes.*

> *"I believe that they should be careful about who is going to have access to our data, to all our data, to all our private things"*.

Finally**,** the participants discussed at length the problems associated with the *interpretation* of the data. It was not so much the worry associated with being monitored, but rather the fear of being 'interpreted', judged on the basis of the gathered information. This very issue gave raise to several doubts. First, it raised doubts about the capability of security officers of interpreting correctly the information received. Second, it raised concerns about the pervasiveness of clichés and stereotypes, that is to say the need to standardize and homogenize people and behaviors in order to match the interpretative scheme of those who are in charge of the security systems. Third, it questioned the real effectiveness of a system where all citizens come to be considered as a potential risk for the security of the state.

5. Technology, Security and Democracy

As previously mentioned, the majority of participants supported the idea of increasing security measure through the adoption of new technologies, but only in specific cases and places, and in any event only within the public sphere. The infringement of privacy in the private and intimate sphere, in contrast, has been consistently described as intolerable. With regards to the latter sphere, the use of invasive technologies can only be accepted in extreme cases, where urgency, gravity are of the highest level and there is no alternative. The use of technologies, in this case, must be justified by serious and unambiguous evidences: *"This is it, it is a violation of your privacy but if it truly is for your security you can't really complain"*.

In the debate, the participants went further and even specified in which cases they would accept the violation of their privacy. First of all, they mentioned gender violence and sexual harassment. In case these technologies may be effective in preventive violence against women, they can be accepted: *"Violence against women, in this sense we ought to put much more effort in terms of security"*. Second, they mentioned ordinary crime and petty criminality, like street violence. In order to prevent crimes like theft, rape, murder, and pedophilia, the use of new technologies was welcome *"The type of criminals that keep committing the same crime, such as rape and pedophilia... these people should be monitored much more intensively"*

Only in the third place of an ideal list of priorities, these technologies were associated to the fight against terrorism. The participants were willing to lose part of their privacy in order to gain more in security in public places as well as in all the places where people form crowd, like football stadiums, concert halls, train and bus stations, airports and shopping malls.

> *"I believe these measures are appropriate for international crime and terrorism, this is clear... I mean that the citizen should know that these measures may occasionally be annoying, that there are people who cannot stand them, cannot stand being controlled in the airport, and so on, but it is for their benefit. If there was no terrorism, all of that would not be necessary"*.

Actually, the participants suggested alternative ways in which these technologies would be useful, i.e. the monitoring of elderly people, children and people that suffers from serious handicaps: *"It could also be positive for the old people who live alone at home, positive because they are looked after and will not die alone"*.

All participants expressed concern that the effort in increasing security measures would be concentrated only against terrorism and only in places considered as sensitive targets, leaving

the citizens unprotected and vulnerable in other places and in relation to other types of crimes. In this respect, they fear that there is a new "elite" security that is emerging and considers terrorism as the main danger, as opposed to the concept of security normally shared by ordinary people, which focuses more on other types of danger and crimes connected to daily life. The latter concept places less emphasis on the threat of terrorism because it acknowledges not only its changing nature but also the ability and creativity of the terrorists in elaborating new strategies of attack and violence.

Last but not least, some participants expressed concerns about the impact of new security technologies in terms of their potential to generate social discrimination and/or stratification.

> *"No, I believe that sometimes there is a risk of confusion... I know what happened to me when I went to Miami, I had some problems, especially after the 11th of September... they stop me all the times to ask for my documents, to ask whether I really was Spanish and put me in the cabin to check my luggage. Why was that so? Because I look like an Arab or a Mexican... you can feel badly when these things happen... I mean just because of your physical appearance, they affect your privacy and there is no respect for the people and this doesn't really prevent a massacre"*

Although positive about participatory processes of development and implementation of the new technology, the participants assigned more importance to transparency of information and effectiveness of general rules than to direct participation. In other words, in their ideal priority list, the introduction of new security technologies should be carried out 1) with absolute transparency 2) with the highest level of information possible 3) in a clear framework of rules, procedure, controls and sanctions 4) under the control of the State and the judicial authority and 5) with a wide participation of various social actors.

With regards to public participation, the question on who was expected to participate gave raise to a debate characterized by the emergence of two positions. Some participants addressed the question in a positive way, trying to identify who was supposed to participate, whilst other participants preferred to focus on who was *not* supposed to participate. Whilst there was general agreement on the crucial importance of involving experts, consumer organizations and human rights associations, the debate was far more fragmented when addressing the participation of ordinary citizens and of the politicians.

Arguing that the lay public should indeed participate, some participants specified that only the participation of ordinary citizens will ensure that their interests would be respected and their concerns taken into account. At the end of day, as they say, it is the citizens who have to live with these technologies on a daily basis: *"Because, if things go wrong these are the people who are going to suffer from their consequences, both negative and positive ones"*.

In contrast, the participants who expressed skepticism the participation of ordinary citizens argued that it would be impossible for them to reach a viable consensus: "(...) *because I believe that the ordinary citizen... that we would never reach a consensus on these measures, never"*. In addition, they also argued that the lay public is not well informed or prepared to effectively participate in the development and implementation process.

> *"I believe that these should be highly qualified people, or maybe the city council, or those who will actually be responsible for their operation in the city or in the*

specific place where these technologies are going to be used... because I believe that the citizen will never be (qualified)".

In fact, the participation of state representatives, and more specifically of politicians, was more controversial. Some participants argued that it is the State that has to guarantee the protection of privacy and the correct implementation of these technologies and therefore its participation is absolutely necessary: *"I believe that they should accept this, not only the States but also the regions and the European Union, but these (technologies) should be regulated with very strict directives* (...)." Yet, other participants felt very negative about this proposal and voiced a deep skepticism about the real value and capability of their political elite: *"Maybe it is better to keep the politicians out, maybe they should not express their opinion because they may give a very personal opinion, it would be better to have others who might be able to see our interest in a more objective way."*

In any event, the participants clearly stated that banks and multinational corporations should not be involved in the participatory process. In general, all the participants shared a very negative opinion of these organizations for they were perceived as permanently seeking their own interests without ever taking into account the social interest at large: *"Banks are not monitored, telephone companies are not monitored. Only terrorists are monitored, but there are other forms of terrorism, like the one operated by banks charging far more than they should, that are not monitored"*

By the same token, the large majority of participants also agreed on the absolute necessity of introducing clear regulative and participative frameworks, in which not only the State and the lay public, but also the judicial system is expected to play a significant role. In fact, the judges are expected to have the final word on the actual implementation and correct utilization of these technologies: *"When there is need to violate the privacy, this should be always authorized by a judge, who has to decide the methods as well as the appropriate time and space constrains"*

6. Conclusions and Recommendations

In all the groups, the assessment of the positive aspects of these technologies followed an individualized approach. In other words, the technologies were positively assessed as long as they were perceived as directly providing personal benefits. In general, there was a remarkable consensus on the need of additional security related to some aspects of ordinary life, such as circulation in the streets, in commercial areas and shopping malls, and the protection of on-line data. In the balance between security and privacy, however, the groups generally reached a consensus on the adoption of these new technologies only in relation to specific cases and issues.

General consent was granted only upon the condition that these technologies would be used for specific crimes, in specific contexts, in proportion to the gravity of the crimes, and for prevention purposes. In addition, all the participants agreed that these technologies should always be employed under specific guarantees, given that it is necessary to regulate in details both their development and their implementation, on a case by case basis. An unregulated implementation of these technologies would produce a loss of confidence in the framework of law and rights of the democratic states. In other words, if concern for security turns into an

obsession, this would inevitably cause the end of the achievements so far obtained by western civil society.

The participants acknowledged that, due to terrorism at a global scale and to the increase of general crime, it is necessary to use new security technologies, even if this change would imply a reduction in terms of privacy right and protection of intimacy. Yet, they detected an over-emphasis on terrorism at the expenses of other risks that they perceive as more imminent and familiar. In fact, they showed resistance against the process of de-territorialization that terrorist threats are imposing on the general approach to security. The participants looked determined in making sure that the introduction of new security technologies should only occur in exchange for a real and *general* security enhancement in relation to concrete and identifiable risks.

Moreover, the participants clearly specified that they are not willing to accept the use of these technologies for any other purpose, especially commercial and political ones. They were aware that 'fear' is a very powerful and rentable feeling in both economic and political terms; therefore they vividly expressed their concern of falling victims of abuses, occasionally speaking of an authoritarian slippery slope. Second, the participants pointed to the difficulty of assessing when a behavior or an attitude of the citizens may be defined as suspicious. This confirms the gradual blurring of the boundary between innocent and guilty suggested by Beck: citizens feel that anyone can come to be included in the grey area of "suspects".

Third, there was special concern about the profile of those people in charge of monitoring the citizens, which usually urged citizens to claim a strict form of institutional control of the 'controllers'. The participants were clearly aware that errors may spring not only from the limits of the technologies but also from the limits of the people who operate with these technologies. As a consequence, the participants claimed the necessity of clear rules and reliable mechanisms of sanction in case of human errors. As we have seen, the professional and moral profile of the operators of these technologies has actually been a very important issue throughout the debate. Interestingly, the sense of vulnerability provoked by security threats is actually overlaps with the threats posed by a wrong application of monitoring technologies

In sum, the participants, with different levels of support, seemed to accept the need to introduce new security measures, even if these technologies may seriously affect their own privacy. Yet, their acceptance does not encompass a-critically all the technologies and does not extend to all circumstances. Consistently with the results proceedings from the questionnaire, the participants made clear that the introduction of new security technologies should be a) gradual and transparent and b) occur always in a context of clear rules and widespread information. In addition, the introduction of new security technologies c) should be focused on specific cases and places d) should be proportionate to the danger and the situation and, finally, e) should affect the private sphere of intimate life as little as possible. In one case, a participant made this point explicitly, suggesting that there is no point in introducing CCTV cameras when it would be sufficient to have more light in the streets. In fact, in several occasions, the participants have expressed their need of feeling safer but they also specified that it was not a question of 'more' security but of 'better' security.

Confirming the importance of the process of individualization, the groups generally achieved common positions only whenever the adoption of new technologies could be left to individual choice. In other words, in their opinion each citizen, whenever possible, should autonomously

decide when, where and to what extent, make use of these new security and privacy technologies. The idea of having tailor-made technologies was considered as the ideal solution to strike a viable balance between improving security and respecting individual privacy.

However, the most interesting and, in a way, unexpected result was that citizens seem to be aware of the political implications associated with the introduction of new security technologies as well as of the political role played by the discourse on security. They explicitly mentioned that the over-emphasis of terrorist threats and national security may serve two functions: diverting attention from other relevant political issues as well as spreading a sense of vulnerability and fear in order to encourage higher level of obedience and self-sacrifice.

This last issue brings us back to Beck's argument on transformation currently affecting the social, political and economical system based on the *Homo Œconomicus*. For a long time, western society relied on a doctrine of utilitarian individualism in social and economic terms and on the democratic political system in political terms. These two dimensions found in individual liberty its essential cornerstone and relied on individual rationality for the pursuit of their own self-interest as the basic driving force sustaining individual behaviour in social, economic and political relations. This seems to be no longer the case.

Within the framework of a globalized risk society, the declaration of the war on terror and the subsequent introduction of new doctrines of internal and external security – which led to the implementation of a new foreign and security policy, focused on pre-emptive strike and permanent internal vigilance and control – seems to be changing the very basis of modern capitalist society. Current national governments, with a different degree of intensity, seems to encourage the reconstruction of citizen identity as potential and permanent targets of unforeseeable though real, unpredictable an yet pervasive safety risks; and as members of a collective entity permanently under security threats. Individuals acting in response to personal or collective dangers and threats, whether real or simply perceived, are more malleable to political calls for action, obedience, self-sacrifice and manipulation. In this respect, fear seems to be politically more rentable than the individual pursuit of economic self-interest.

Are we then moving from a society based on the *Homo Œconomicus* to a society based on the *Homo Metuens*? If this is the case, there is a further implication that should receive due attention. Individual self-interest, to a certain extent, is a self-sustaining motivational force of individual behaviour, which keeps driving individual action within the main boundaries represented by ethical, legal, political and cultural constraints. In contract, fear and anxiety, though more responsive in the short terms, are not self-sustaining in the long run. We all know that fear and terror are very powerful feelings, whose power though tend to decline as time passes, unless it is constantly regenerated by punctual events or threats. Fear, as a socio-political driving force, needs to be periodically reinforced to maintain its efficacy and avoid natural waning. As suggested by Žižeck (2003), this may actually force national governments, and political actors in general, who wants to exploit human fear as a political motivational mechanisms to intervene periodically in the public sphere in order to reinforce the sense of vulnerability, the potential threat of the enemy and the ubiquity of risks and dangers in order to nourish human obedience and self-sacrifice. As a consequence, the public and private discourse on risk and terror is likely to enter a spiral of ever-increasing growth in terms of space, time and intensity that runs the risk of leading a new transition from the *Homo Œconomicus* to the *Homo Metuens*, into a society where democratic values and mutual trust as we were used to experience them will be deeply transformed and, perhaps, lose political relevance.

References

Beck, U. (1992), *Risk Society: Towards a New Modernity*, London: SAGE.

Beck U. and C. Lau (2005), "Second Modernity as a research agenda: theoretical and empirical explorations in the meta-change of modern society" in *British Journal of Sociology*, vol.56, no. 4, 525-557.

Beck U. (2002), "The Terrorist Threat: World Risk Society Revisited" in *Theory, Culture and Society*, vol. 19, no. 4, 39-55.

Beck U., W. Bonss and C. Lau (2003), "The Theory of Reflexive Modernization – Problematic, Hypothese and Research Programme" in Theory, Culture and Society, vol. 20, no. 2, 1-33.

Bowyer K. W. (2004), "Face recognition technology: security versus privacy" in *IEEE Technology and Society Magazine*, spring 2004, 9-20.

Duffield, M. and N. Waddel (2006), "Securing Humans in a Dangerous World" in *International Politics*, No. 43, 1-23

Ekberg M. (2007), "The Parameters of the Risk Society" in *Current Sociology*, vol. 55, no. 3, 334-366.

Erickson J. and G. Giacomello (2006), "The Information Revolution, Security, and Internatioal Relations: (IR)relevant Theory?" in *International Political Science Review*, vol. 27, no. 3, 221-244.

Heng Y. (2006), "The 'Transformation of War' Debate: Through The looking Glass of Ulrich Beck's World Risk Society" in *International Relations*, vol. 20, no. 1, 69-91.

Jain A. K., A. Ross and U. Uludag (2005), Biometric Template Security: Challenges and Solutions, web-source available at: http://biometrics.cse.msu.edu, last accessed June 2008

Lash, S. (2001), "Non-Linear Individualization" in U. Beck and E. Beck-Gernsheim (eds), *Individualization*, London: Sage.

Levi M. and D. S. Wall (2004), "Technologies, Security and Pirvacy in the Post-9/11 European Information Society" in *Journal of Law and Society*, vol. 31, no. 2, 194-220.

Liberatore A. (2007), "Balancing Security and Democracy, and the role of Expertise: Biometrics Politics in the European Union" in European Journal of Criminal Policy, no. 13, 109-137

Luhmann, N. (1993), *Risk: a Sociological Theory*, New York, Aldine de Gruyter.

Mythen G. and S. Walklate (2006), "Criminology and Terrorism: which thesis? Risk Society or Governamentality?" in *British Journal of Criminology*, no. 46, 379-398.

Shearing C. and L. Johnston (2005), “Justice in the Risk Society” in *The Australian and New Zealand Journal of Criminology*, vol. 38, no. 1, 25-38.

Spence K. (2005), “World Risk Society and War Against Terror” in *Political Studies*, vol. 53, 284-302

Strickland Lee S. and L. E. Hunt (2005), “Technology, Security and Individual Privacy: New Tools, New Threats and the New Public Perceptions” in Journal of the American Society for Information Science and Technology, Vol. 56, No.3, 221-234.

Waever O. “Securitization and Desecuritization” in R. Lipshutz *On security*, NY: Columbia University Press, 46-86.

Weiss C. (2005), “Science, Technology and International Relations” in *Technology in Society*, no. 27, 295-313.

Žižeck S. (2003), “Paranoid Reflections” in London Review of Books, 25 (7), 9.

Zureik E. (2004), “Governance, Security and Technology: the Case of Biometrics” in *Studies of Political Economy*, no. 73, pp. 113-137.

Privacy, Public Life and Security Technologies – An Urban Perspective

Holger Floeting
German Institute of Urban Affairs, Dpt. of Economy and Public Finance
floeting@difu.de

1. Introduction

Urban security is the subject of increasing public debate. Despite a current lack of integrated urban security policies with dedicated security resources in Germany, new urban security regimes are developing to meet specific threats. The discussion on urban security adds another aspect to the discussion on privacy and security by focusing on the triangle of privacy, public life and security.

The paper contributes to the debate of real versus perceived security gains from technologies by describing the triangle between privacy, public life and security and its implications on urban security regimes, highlighting examples for ICT-supported security technologies and technological-organizational convergence in an urban setting, analysing governance patterns of ICT supported security technology based municipal safety and security approaches and sketching the future of city life under new ICT supported urban security regimes.

2. Privacy, public life, security and security technology in urban policy

Why is the relationship between privacy, public life, safety and security matters and the adoption of security technologies an urban policy issue?

First, privacy is a societal value and a fundamental right for every human being. This fundamental right seems to be increasingly endangered by security demands.

Secondly, the relation between privacy and public life has subtly changed. Boundaries between the individual private sphere and public life became blurred not only figuratively but also literally. Lifestyles have changed dramatically driven by information and communication technologies in the last 20 years. Internet access in private households increased dramatically. Thus public life expanded into the private sphere. Access to mobile communication is nearly ubiquitous in urban areas in Germany. Thereby the individual sphere appeared in public places like streets and squares, train stations and airports etc. An amalgamation of private and public domain is taking place in public places.

Thirdly, with the extensive diffusion and use of ICT the amount of generated personal data has skyrocketed. New technological options offer almost endless opportunities to transmit and store data at rock bottom prices. In combination with an apparently increased demand for safety and security notably in urban environments the request for pre-emptive safety and security measures has increased constantly.

Fourthly, evidence suggests that there is an increase in more careless handling of personal information by both sides: individual people and institutions not accounting for storage and circulation options of networked ICT.

Fifthly, most of these phenomena take place in urban settings. Urban areas are centres of knowledge. That is the reason why urban centres are most affected by the use of ICT. They are also hubs of the new information infrastructures. ICT users are concentrated in these areas. Knowledge based industries are concentrated in urban areas. Here you can find innovative settings for developing new ICT services as well as the contents to transmit by using ICT. Decision makers are located primarily in urban areas. They use ICT themselves, but they also have to decide on the framework conditions of technology development. Therefore urban areas are locations of industrial-political decisions which define the technological future. Last but not least, urban areas with their densely built-up areas and sophisticated infrastructures are extremely vulnerable for terrorist attacks. This threat is a main driving force for diffusion and adoption of security technologies even though security technologies aim at combating crime, deviant behaviour and incivilities in general.

3. ICT supported security technologies in urban areas

The security technology sector offers an array of solutions equal to the complex task which are being implemented in municipalities or may be introduced in the future. Security authorities are willing to resort to technology, particularly when faced with imminent or suspected threats. In most cases this occurs before thorough analysis has been performed or integrated action plans synergizing technology, strategies, concepts and non-technological measures have been devised. Such solutions appear to appease technology users, or at least decision-makers, who are at least able to demonstrate the ability to react in critical situations, and technology providers who "portray an immature technological application as a panacea" (Lenk 2006, p. 2).

The security market is booming. The German federal government, will spend approximately 3.5 billion euros in 2008 on internal security not to mention the expenditures of the “Länder” and the municipalities. The Federal Criminal Police Office (Bundeskriminalamt) spends about 13 percent of its budget on ICT (Bundesregierung 2007). The market volume only for electronic safety features and equipment in Germany accounted for 2.3 billion euros in 2006 (ZVEI 2007). These figures clearly show that the employment of security technologies and urban security restructuring not only involve security considerations, but are also economically motivated.

Safety and security features and equipment in urban areas cover a wide range of areas of application including:

- information systems (for players and residents),
- expert systems (decision support),
- workflow management systems (to facilitate cooperation between a disparate cast of players),
- help systems (for players and citizens),
- monitoring networks (information gathering and early warning),
- GIS applications (spatial analysis and forecasting potential and imminent disasters),
- data mining (to generate detailed profiles),

- augmented reality (to aid decision-makers and their support staff) and
- ubiquitous computing (comprehensive networking) (Floeting 2007).

The following sections expound upon only a few examples of new security technology application in municipalities. The cases described below focus on "visible" front-end applications for public and private spaces. They often represent common standard more than latest technology. They illustrate how commonplace security technologies already are in spheres which do not incontestably fall under "internal security".

3.1 Video surveillance

The topic of video surveillance is not new to municipalities. It is considered "the most significant innovation for internal security in cities" (Wehrheim 2004, p. 23) in recent years. Video cameras are widely used to monitor traffic. Video surveillance systems have also become an established component of facility security (for government agencies, stadiums, public transport etc.). For years now video surveillance systems have been used to prevent crime on city streets and in public spaces, e.g. to police drug-related criminality. This development was spearheaded by British municipalities, some of which have proceeded to implement CCTV systems extensively in shopping streets, busy public places and elsewhere so individuals can be traced throughout larger areas of cities.

Surveillance of this sort can be automated with the support of biometric and behavioural characteristics. One possible use would be "filtering out" people who are considered likely to do property damage (e.g. graffiti tagging) on the basis of route tracking (Floeting 2007).

In Germany video surveillance was first used as a tool to monitor urban public spaces in Leipzig in 1995 (not considering the time before 1990, when video surveillance of public spaces was part of the repression system in the GDR). There has been no attempt to establish a nationwide surveillance scheme in Germany like the one in the UK although after 2000 *Länder* police law amendments facilitated broadening of video surveillance in public places. Cities argue that video surveillance activities should be restricted to crime hotspots. Surveillance can complement other crime prevention measures, but is not a substitute for them (DST 2004, p. 5). Currently in about 40 municipalities in Germany video surveillance is used to monitor crime hotspots (Hempel 2008) in areas like the Reeperbahn in Hamburg, a redlight and entertainment district, areas around train stations (e.g. Böblingen, Leipzig) etc. The number of permanently (for a specific period of time) installed video cameras is estimated at 500,000. Video surveillance has only been used sporadically to monitor crime in German cities. For the most part crime-ridden areas were observed with two to three cameras (Wehrheim 2004, p. 23). The London terror attacks, the train bombs found in North Rhine-Westphalia and daily reports of vandalism and violence on public transport and in public spaces in general have spurred further debate on substantially broadening the scale of video surveillance (Floeting 2007).

Because constant surveillance of public places often leads to profound invasions of personal privacy (the right to one's own image, the right to informational self-determination) its implementation is limited; private monitoring of public spaces is restricted, time limits have been set for data storage, the use of hidden cameras is prohibited and notices of surveillance activities must be posted. The German Federal Constitutional Court (Bundesverfassungsgericht – BVG) decided that municipalities are not permitted to set up CCTV schemes in public areas

if this infringes the right of personal information of persons randomly passing there.[1] Nonetheless, there continue to be grey areas, infringements and inconsistencies which have incited public debate on video surveillance. The use of surveillance data in borderline cases continues to be a hot topic.

Video surveillance data analysis has proven particularly effective in solving crimes. It is used more and more to identify offenders (e.g. following the attacks in the London Underground, in combating ordinary crimes, vandalism etc.). A wide range of opinions have been expressed regarding how effectively video surveillance deters crime. Its preventive impact in high crime areas is commonly mentioned as a positive outcome along with its provision of evidence for criminal prosecution. Measurable crime reduction in areas monitored with CCTV is sometimes offset by increased crime rates in other areas, the so-called displacement effect. Analysis of video surveillance evaluations showed that CCTV "can be most effective in reducing crime in car parks"(Welsh/Farrington 2002: 45). Compared to that the effect on crime of CCTV schemes in city centers, public housing areas and public transport was rather small (Welsh/Farrington 2002). Nevertheless there are very effective isolated cases like the CCTV scheme in the city center of Mannheim where the crime rate was reduced by up to 60 percent in the last six years when video surveillance was in place (Stadt Mannheim 2008). In fact video surveillance was so successful that it is suspended now because federal legislation in Baden-Württemberg allows only for regional and temporary video surveillance as long as there is a crime hotspot. Currently politicians in Germany (e.g Baden- Wuerttemberg, North Rhine-Westphalia) are discussing an extension of video surveillance by abolishing the initially limited time period of CCTV schemes.

The scale of surveillance has already expanded significantly in recent years and will continue to grow in the mid-term. Whereas there are still significant differences in the diffusion of CCTV in public spaces between different European countries (with a leading position of the UK), the diffusion of CCTV in private spaces (offices, shopping malls etc.) look pretty similar in Europe now. In addition to the proliferation of cameras in public spaces, various surveillance techniques are being networked, and private und public security measures are being coordinated, e.g. to create security alliances (cf. Hempel 2003). Unlike the UK in Germany meta evaluations of CCTV schemes are still missing, to some extent even individual evaluation of CCTV schemes is missing. Experts complain about a "reflex-like call for an extension of video surveillance" which has "not triggered a discussion about the limitations of the technology" (heise online news 2008).

[1] In the summer of 2005 the city of Regensburg opened a monument to the former synagogue on a city center square to the public, which soon became a target of anti-Semitic attacks. The city set up surveillance cameras to deter or capture offenders. A lawyer who passed the site regularl claimed that his right to privacy was being infringed and sued the city to remove the cameras. After having lost in the first two rounds he succeeded at the German Federal Constitutional Court (Bundesverfassungsgericht, Pressestelle, Pressemitteiluing Nr. 31/2007, 20.3.2007, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg07-031 (20.3.2007); BVerfG, 1 BvR 2368/06 vom 23.2.2007, Absatz-Nr. (1 - 58), http://www.bverfg.de/entscheidungen/rk20070223_1bvr236806.html).

3.2 Biometric access systems

Using biometric identification in counterterrorism has been discussed frequently in recent years. The debate centres on integrating biometric data in identification documents and using biometric traits for identification and access control. The number of operational biometric ID systems in Europe has skyrocketed from around 8,500 (1996) to over 150,000 (2004) (European Commission Joint Research Center – JRC, cf. Horvath 2005). The biometrics industry is expected to grow considerably. Unfortunately, no official revenue or employment statistics are kept for this sector. It is difficult to distinguish exactly what proportion of security technology implements biometrics, and the companies involved tend to have prohibitive information policies (cf. Petermann/Sauter 2002, p. 6). We must therefore rely on market studies conducted by interest groups and private institutions. In 2004 the entire biometrics market in Germany was estimated at 12 million euros. Large federal government contracts are expected to push market volume to 377 million euros by 2009 (SOREON 2004, cf. http://www.heise.de/newsticker/meldung/48560). Despite the stated reservations, the figures suggest that the market is indeed still maturing. As is often the case when new technologies are first introduced, revenue forecasts are very optimistic. It is also evident that large government contracts have been driving the market (Floeting 2007).

Biometric systems tested to date use facial recognition[2], fingerprinting[3] and iris scans[4]. Forensics identify people using DNA characteristics.[5] At the end of 2006 the Federal Criminal Police Office (Bundeskriminalamt) only stored 542,000 DNA data records from accused and convicted persons and crime scene prints. Using several kinds of biometrics in parallel (to augment safe recognition) multiplies the privacy problem.

An array of unsolved problems remains. Some individuals cannot be detected with fingerprint and iris recognition because their traits cannot be recognized or are not sufficiently distinctive. With age, recognition methods become less reliable and some occupations (e.g. jobs in which finger injuries are common) hamper biometric recognition. Moreover, conditions at the time of recognition (e.g. lighting during facial scanning) can interfere with the system. Lastly, these systems are feared to have too many security loopholes, e.g. fingerprint recognition (Bundesdatenschutzbeauftragter 2005, p. 47 f.). In addition, no bioethical frame of reference has been established for the development and use of biometric technologies. Discussions on the acceptability of biometric technologies have focused mainly on cost-benefit aspects and security issues (BITE 2005).

The notion that such access systems are only employed in high security areas and at border control points is erroneous, as the entry system for Hanover Zoo season ticket holders illustrates. People wishing to subscribe to the zoo must first supply personal information which

---

[2] Facial recognition systems analyze specific facial features from a scanned image. The individual traits analyzed are used to create a biometric signature. Two and three-dimensional facial recognition systems are available.

[3] Finger printing systems generate individual fingerprint images. Various types of sensors are employed (pressure, ultrasonic, optical, thermal, electric and capacitive). The image is used to detect characteristic peculiarities (arches, loops and whorls) which are compared with existing data.

[4] Iris recognition systems illuminate the eyes of the person being identified with infrared light to create a high-resolution, near-infrared image which is then examined for specific features (corona, depressions, muscle fibres, pigment spots, scars, radial furrows, striations). Idiosyncratic traits are then used to generate an iris code which is compared to records in a database.

[5] Deoxyribonucleic acid is a nucleic acid stored in cell nuclei which forms a double helix and contains the genetic instructions for biological development.

is recorded in a ticketing system. A digital photo is taken and saved the first time the ticket holder visits the zoo. Digital photographs are taken before entry on every subsequent visit and are compared with the stored data. Visitors may only enter after they have been positively identified. With more than 71,000 visitors, this represented the largest application of biometric identification in Germany's service sector in 2004 (DStGB 2003, Glitza 2004, Schiffhauer 2004).

Municipalities could install biometric entry systems in places like museums and sports venues. Numerous other applications in the realm of security are conceivable (Floeting 2007).

3.3 RFID

Radio frequency identification (RFID) is microchip technology which enables contact-free data transfer. RFID systems include an antenna, a transceiver, a transponder and radio frequency technology. They can be employed to: recognize objects, authenticate documents and commercial goods, optimize processes, i.e. automate logistics, support access control and track vehicles and monitor the environment etc.

Transponder systems are not entirely new. They have been used to identify animals for around 20 years. Due to significant advances in silicon chip technology and radio transmission, and especially due to the improved integration of the two, RFID has become a focus of public debate. It is superior to other technologies employed for similar purposes:

- It offers a much broader range of features for access control technology than standard smart card and magnetic stripe systems. Non-contact data transmission is user-friendlier (no waiting periods, active registration process etc.).
- In the logistics field, bulk processing can replace the time and labour consuming individual registration of goods. This improves operational efficiency and increases resource utilization rates. RFID also has security advantages (e.g. asset tracking).
- Branches with high security requirements and extensive verification procedures benefit most from cost reduction (e.g. logistics and waste management companies).
- Businesses with self-contained supply chains (e.g. retailers) also expect to profit from this technology. In flow structures of this sort RFID transponders, which are still relatively costly, can be used repeatedly and continually (BSI 2004, p. 85 f.).

Cities are applying RFID technology to an ever greater degree. RFID applications already abound in public transport. Because about a fifth of ticket costs are spent to manage ticket sales, radio frequency identification is appealing to transit companies. Adopting this technology is expected to lower costs and improve transport operations. Germany's first project with contact-free cards was introduced in the mid-1990s (Cap 2005).

RFID applications in urban settings are now used in healthcare, facility management, waste management, public libraries etc. (Floeting 2007).

A major worry regarding RFID technology is that personal data may be manipulated because the processing stages lack transparency. Some systems allow data access from metres away. Both RFID and readers can be inconspicuously embedded in everyday objects. Data protection

concerns are reinforced by awareness that "identifying individuals, including linking this technology with video cameras, […] has already been tested on the market" (Bundesdatenschutzbeauftragter 2005, p. 46). A number of everyday viability issues remain. A temporary deactivation of RFID chips might be a solution for challenges in privacy. There are severe problems concerning privacy using RFID technology in its current form. The main threat to privacy lies in the combination of RFID and database technologies. Threats concerning privacy are tracking and profiling in certain environments (shops, librarys etc.), personal related tags (e.g. IDs), tag presence spotting, using a combination of tag information and following a unique ID (Hennig/Ladkin/Sieker 2004).

4. Technological-organizational convergence

New security technologies can be utilized in a variety of ways in urban areas. The combination of a range of technologies, such as video surveillance, biometric profiling and non-contact data transfer is enabling the development of complex identification, entry and surveillance systems and by that combination multiplies the risks concerning privacy. These schemes can control access to and use of certain areas (city centres, local public transport, embassies, ministries, government agencies etc.) and larger parts of a city. Convergent technology systems like these are already in place.

Economic changes (e.g. drop-off in prices of computer memory) and technological developments (e.g. higher capacity of storage media) are making it easier to manage data. Storing information without specific justification or purpose is becoming an increasingly popular precautionary measure (particularly in security circles). It is also maintained that the public is more inclined to allow their personal data to be filed, possibly as a trade-off for heightened security. On the basis of this assumption, there have been efforts from some quarters to facilitate the process of gaining ex post access to data which was originally gathered for different purposes. The debate in Germany on using road toll data to combat crime and terrorism demonstrates the issues at hand. The gradual spread of the practice of using data retroactively for objectives other than those originally intended is one of the main reasons for public opposition to storing personal data in any form.

On the one hand, we must take full advantage of all technologies which can be employed to contain threats. On the other hand, the growing practice of collecting personal data and information that can be traced back to individuals within their particular urban setting and the possibility to link this data will take surveillance to a whole new level. Organizational as well as technical convergence has a particular role to play in this domain. The opportunity to link data, combined with factors such as the increased overlapping of internal and external security countermeasures and a desire to assess the situation comprehensively based on the available facts, will make it possible to develop ever more detailed profiles of individuals. Without wanting to dramatize the situation by conjuring an image of the "transparent citizen", technical-organizational convergence will make it easier than ever to obtain details on private citizens. Closer integration of technical and organizational resources will also increase the danger of data being misappropriated at a later date (Floeting 2007). Hence measures to balance privacy and surveillance should address not only single applications but focus across applications.

5. Future of public life under new ICT supported urban security regimes

The use of information and communication security technologies involves dangers and potential benefits which must be considered and weighed up. Surveillance technology, for example, has preventative potential as it lowers the detection threshold (e.g. of minor violations and crimes) and of potentially dangerous situations. The subsequent growth in intelligence on particular security matters could theoretically enable early intervention. Empirical findings however, taking the situation as a whole into account, demonstrate that the potential of these technologies is not being exploited and cannot be exploited. On the other hand, there is a danger that surveillance which is focused too heavily on certain areas will lead to exclusion or crime displacement (Floeting 2007).

The implementation of ICT security technologies can improve a city's accessibility if, for example, permanent security measures such as fences, security margins and protection devices are replaced by technological control systems and temporary measures. However, these technologies can also reduce the accessibility of certain city areas if that is the purpose of the system or if its implementation targets certain social groups too heavily (cf. Graham 2005).

It is always difficult to assess the impact of a technology. Security technology, too, can only be properly judged once in a specific application. The growing use of security technologies must be considered in the context of real and perceived threats and the security regime which has been set up to counter them.

Safety matters are a challenge for urban environments. The changing nature of the threat, the increasing use of security technology in particular parts of the city and the growing significance of security issues for city life could have a variety of repercussions. These include a fundamental shift in the image of cities, the long-term transformation of urban architecture and space and adjustments in the use of urban sites (Floeting 2007).

5.1 Cities as unsafe places

The public may increasingly view cities as unsafe places, giving rise to a new type of "urban fear". Cities are comparatively "unmanageable areas" and are therefore suspected of harbouring every type of security threat: from "common criminals" to terrorists planning attacks. These fears are already being voiced in international urban studies literature[6]. There is a very individual fear of crime. The objective crime rate is often low, while people may expect it to be at a high level.“ Mixing up deviant behaviour, incivilities, crime and terrorism in the public debate on urban safety and security prepare the ground to asses urban environments as unsafe places. Perceived safety of a certain location seems to become a locational factor for the settlement of companies and citizens. To be reckoned a high crime area may lead to a downward spiral in economic and social development of a neigbourhood. Therefore urban planning has to focus more and more on safety and security measures. It has the opportunity to create a picture of safe and secure places and contributes to make public and private spaces

[6] Cities are especially well suited for furnishing terrorists with anonymity, safe houses and supply depots in order to prepare attacks as well as gain access to potential targets. […] Terrorists can more easily become invisible in overcrowded neighborhoods; they can hide weapons and explosives in obscure places and they can freely conduct themselves in a maze of twisting streets." (Savitch 2005, p. 362)

appear more manageable and to encourage people to use public spaces (Floeting 2007). Privacy issues are weighed up against the necessity to create this „citizen and economy friendly" safe urban environments and often mentioned as price that we have to pay for a safe city.

5.2 Fortification of cities

A growing or lasting threat could lead to public and private places becoming more heavily "armed" through the step-by-step introduction of security measures, security technologies and architectural features which promote safety. First, authorities, the public and investors begin to pay more attention to what happens around, thus creating a kind of informal surveillance system. Then security technology is upgraded and regulations controlling activities in public places are tightened. Fences, barricades and gates are constructed and an "architecture of fortification" begins to distort the face of the city. In security circles, this is referred to as "target hardening" (Oc/Tiesdell 2000). Urban planning has to assess the specific safety and security demands of different locations carefully in order to create lively and attractive public and private spaces. On the one hand a fundamental fortification of urban structures would dramatically constrain urban life and constitute a massive encroachment in privacy issues. On the other hand appropriate implementation and use of security technologies may help to minimize interventions in the spatial structures of urban areas. Surveillance and access control technologies may substitute some structural measures ("intelligence instead of concrete"). In this way security technology offers the opportunity to minimize barriers.

Security considerations may strongly influence town planning - at least at vulnerable locations. This would significantly change the face of city centres where such sites are concentrated (e.g. Berlin or Frankfurt am Main). The solution could be designing and implementing a comprehensive security plan. By looking at London we can see where this development would take us. IRA attacks in the City at the beginning of the 1990s prompted construction of a "ring of steel", like Belfast's. The number of entry points to the financial district were reduced and road blocks were erected, making it possible to temporarily cordon off the area if necessary. Thousands of video cameras were installed, security plans were devised for financial institutions and they were advised to limit the number of entrance points to each building. Buildings were fitted with more security technology and back-up premises of the original sites were created for an emergency. Police patrols increased significantly (cf. Coaffee 2003). Urban planning has to think about what it means to mixed-use areas in the long run, when defined security demands lead to a higher concentration of specific buildings and structures (like office space) in certain "lockable" areas.

Changing security conditions also have implications for the organization of mass gatherings, which have become a favourite tool of modern urban planners in their endeavours to market public space. For example, growing security demands have led to the increasing use of personalized tickets, which can prove extremely inconvenient for the eventgoer and are linked to new needs for privacy. Extensive security measures (road blocks, flyover bans etc.) can also disable large parts of a city (Floeting 2007).

5.3 „Archipelagos of safety“

Supposed "archipelagos of safety" such as shopping malls, business improvement districts and gated communities could proliferate (cf. Wehrheim 2002), leading to the categorization of urban spaces according to their level of security. Polarization would result with areas viewed either as safe or unsafe. Ironically the areas where many people feel confident (controlled private environments like shopping malls) might be the areas where privacy is most endangered. These are the areas with the most CCTV and RFID systems.

A further factor to be considered here is the existence of "undefined areas" which are becoming increasingly common as a result of demographic developments, gradual technological changes and economic restructuring. Due to their frequent recycling, these areas could also be labelled as unsafe.

"Control zones" or "security zones" could be constructed on boundaries of undesirable neighbourhoods. Large cities could develop an island system made up of overlapping milieus (localized poverty milieus, the working, leisure and residential areas of the various lifestyle groups and the milieu of cosmopolitan, highly skilled workers) who strive to control and minimize contact with each other (cf. Wehrheim 2004, p. 26). "Security zones" around "institutions under threat" may be expanded to residential buildings. Depending on the level of security required, temporary entrance restrictions may be imposed on particular parts of a city, combined with technological surveillance of these areas. Measures temporarily restricting access are already in use. These range from police orders (declaring an area off limits to certain individuals) and constructing barricades at events to longer-term entry bans for specific areas. Technological surveillance will considerably extend the feasibility of such entry restrictions and it will individualize access regulations. Access to certain areas in this sense will be a matter of privacy or loss of privacy. Privacy is bargained for easy access. Therefore it will depend on the specific implementation conditions of these technologies and the regulations of their use whether it gives leeway to city dwellers (e.g. by temporarily limiting access restrictions and substituting rigid barriers) or it cuts liberty of action by supporting software sorted urban geographies. Urban planning has to become aware of this possible new inner-urban polarization processes and has to deal with it (Floeting 2007).

The growing use of technological surveillance could transform the nature of public space, ultimately resulting in the loss of certain spaces and the merging of public and private spheres. As the boundaries between the public and the private sphere blur the need for new privacy regulations increases.

5.4 The virtual and the material city

The relationship between material and virtual space could change permanently. The "space of flows" (Castells 1989) could expand significantly. Partly unnoticed, data from everyday activities could be generated, selected and stored. Numerous new links between the expanded "space of flows" and material space could emerge. One example is the spread of data-based admission controls at events (with personalized tickets), for border crossing (with machine-readable ID which automatically detects biometric characteristics) and for security zones (in public and private buildings). The technological developments behind this trend range from individual and isolated applications to complete sustainable networks. The catchwords in this

discussion are "augmented reality", "ubiquitous computing", "pervasive computing" and "ambient intelligence" (Floeting 2007). A networked amalgamation of the virtual and material city constitutes new demands on privacy issues.

6. Conclusion

The public debate on using technology to improve urban security has provoked a very polarized response from decision-makers as well as city residents: security technology is either demonized or uncritically espoused as the solution to all the security challenges facing the city. Up until now, the potential benefits and risks of security technology have hardly ever been evaluated in specific contexts. Instead of deciding whether to implement security technology on the basis of vague speculation about its virtues, we should conduct more empirical research into the specific effects of individual security technologies and their collective impact on privacy. Conversely, to achieve this, we must refrain from automatically condemning every move to introduce security technology as an attempt to establish a "totalitarian State". We should continue to explore the risks associated with these technologies - assuming that this dialogue has indeed begun, a point which itself is open to debate - in order to obtain a more balanced assessment of the situation.

In the future, security looms as a vital issue for cities and their residents. Urban security regimes are developing - more in response to events and ad hoc security demands than as well thought-out, integrative programmes. Urban impact analyses are also necessary to mould this blossoming security regime into an integrated local security policy in the medium term. These analyses should not only resolve urgent issues, i.e. how to manage dangerous and threatening situations and disasters, but must also assess the long-term impact of internal security measures on urban life (Floeting 2007). We have to anticipate bargaining privacy for access to public places, to participate in public life and to make cities and towns safe. Balancing privacy, public life and security and finding appropriate regulations to adopt security technologies in cities and towns is a vital issue for the urban future.

Bibliography

BITE – Biometric Information Technology Ethics (2005): Press Release, January.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2004): Risiken und Chancen des Einsatzes von RFID-Systemen. Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit, Bonn.

Bundeskriminalamt (2007): Facts and Figures, Wiesbaden.

Bundesregierung (2007): Haushalt 2008, Innere Sicherheit, http://www.bundesregierung.de/nn_1264/Content/DE/Artikel/2007/07/2007-07-04-haushalt-2008-innere-sicherheit.html (29.11.2007).

Cap, Clemens H. (o.J.): Anwendungen von RFID Identifikation, slides from the "Smart Cards, Smart Labels, Smart Devices" lecture, Chair for Information and Communication Services, University of Rostock, http://wwwiuk.informatik.uni-rostock.de/sites/lehre/lehrveranstaltungen/vl_smartx/rfid-applications.pdf, 09/05/05.

Castells, M. (1989): The Informational City. Information Technology, Information Restructuring and the Urban Regional Process, Oxford/Cambridge MA.

Coaffee, Jon (2003): Terrorism, Risk and the City: the making of a contemporary urban landscape, Aldershot.

DST – Deutscher Städtetag (2004): Positionspapier Sicherheit und Ordnung in der Stadt.

DStGB – Deutscher Städte- und Gemeindebund (2003): Kommune schafft Sicherheit. Trends und Konzepte kommunaler Sicherheitsvorsorge. Editorial supplement "Stadt und Gemeinde interaktiv", vol. 12.

Floeting, Holger (2007): Can Technology Keep US Safe? New Security Systems, Technological-Organizational Convergence, Developing Urban Security Regimes, Difu-Paper, Berlin, http://www.difu.de/extranet/edoc.php?id=N403LKI7 (25.04.2008)

Glitza, Klaus Henning (2004): Mundwasser gegen einen Hauch von Toll Collect, CD Sicherheitsmanagement 4, 125-129.

Graham, Stephen (2005): Software-sorted geographies, Progress in Human Geography, 29 October 2005, pp. 562-580.

Heise online news (2008): Discussion abaout video surveillance continues, http://www.heise.de/english/newsticker/news/101303 (4.1.2008).

Hempel, Leon (2008): Videoüberwachung in der kommunalen Sicherheitspolitik. Lecture at the German Institute of Urban Affairs, Berlin 22.4.2008.

Hempel, Leon (2003): Verdrängen statt Vorbeugen, in: Telepolis, 15/01/03, http://www.heise.de/tp/r4/artikel/13/13928/1.html, 09/05/05.

Hennig, Jan E., Ladkin, Peter B., Sieker, Bernd (2004), Privacy Enhancing Technology Concepts for RFID Scrutinised, Bielefeld, RVS-RR-04-02, 28 October 2004

Horvath, John (2005): Prepare to be scanned, in: Telepolis, 02/08/05, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20635&mode=print, 13 November 2006.

Lenk, Klaus (2006): Öffentliche Risikovorsorge und gesellschaftliche Sicherheitsbedürfnisse als Gegenstand der Politik. Lecture given at the German Association of Towns and Cities and the Alcatel SEL Foundation symposium on "Municipal Security Communication Systems", 31 May 2006, Berlin.

Oc, Taner, and Steven Tiesdell (2000): Urban design approaches to safer city centers: the fortress, the panoptic, the regulatory and the animated, in: J.R. Gold and G. Revill (eds.): Landscapes of Defense, Upper Saddle River: Prentice Hall, pp. 188-208.

Petermann, Thomas, and Arnold Sauter (2002): Biometrische Identifikationssysteme. Sachstandsbericht, Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), Arbeitsbericht Nr. 76.

Savitch, H. V. (2005): An Anatomy of Urban Terror: Lessons from Jerusalem and Elsewhere, Urban Studies 42 (3), March, pp. 361-395.

Schiffhauer, Nils (2004): Hinter dem Spiegel geht's weiter, in: GIT Sicherheit + Management 12, pp. 12-13.

SOREON Research (2004): The Biometrics Market in Germany 2004-2009.

Stadt Mannheim, Fachbereich Sicherheit und Ordnung (2008): Videoüberwachung im öffentlichen Raum, http://www.mannheim.de/io2/printView/webseiten/politik/aemter/fb31/a-z/videoueberwchng_de.xdoc (25.4.2008).

Wehrheim, Jan (2002): Die überwachte Stadt. Sicherheit, Segregation und Ausgrenzung, Opladen.

Wehrheim, Jan (2004): Städte im Blickpunkt Innerer Sicherheit, in: Aus Politik und Zeitgeschichte, no. B44, pp. 21-27.

Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI) (2007): Enormer Schub für elektronische Sicherheitstechnik – Höchste Wachstumsrate seit 2001 , https://www.zvei.org/fileadmin/user_upload/Initiativen/ARGE_Errichter/Presse/Pr_2007-055_Markt_Sicherheitstechnik.pdf (14.6.2007).

Privacy in The Polippix Project

Niels Elgaard Larsen,
IT-Political Association of Denmark (IT-POL)
elgaard@agol.dk

1 Privacy Enhancing Technologies are not enough

We do not believe that the invasion of privacy is primarily caused by design or implementation errors that can be fixed by performing Privacy Impact Assessments or adding Privacy Enhancing Technologies.

The threat to privacy is mainly caused by centralized gathering of increasingly detailed personal information. Once our personal data is stored and handled by the state our privacy is compromized no matter how the systems are designed and implemented.

To allow citizens more privacy, we have to design systems that are decentralized and require less personal information. For example it should not be necessary to identify yourself when using public libraries (you could still pay a deposit to make sure you would return a book) or medical services (it should be possible to prove that you were covered by health insurance without revealing your identity).

Our personal freedom is threatened by the vast amount of personal information we are forced to hand over to the state just to be citizens, make an income (and pay taxes), receive medical care, get an education, etc. But it is also threatened by leakage of personal information that we are not formally required to release. The latter is the focus of the Polippix project.

Privacy Enhancing Technologies are not enough. We need Privacy Guaranteeing Technologies.

2 Trusting the state

In the view of many actors in the public debate, citizens are too technically challenged to be responsible for their own personal privacy. Therefore the state must do it for them.

2.1 Case: Eboks

In Denmark, all citizens can get a free state sponsored Digital Signature.

Public offices, employers, banks, etc want to save money by replacing paper-mail with electronic “mail”. They could just encrypt documents using the public key of the recipient and send it as an email. But the general opinion is that Danes cannot be trusted with receiving encrypted email.

Instead, they use a service called Eboks. Eboks is a centralized database that receives personal electronic mail for 1.5 million Danish citizens. To read the mail, the citizen can log in using a digital signature, find the new message, download it as PDF-file and view the PDF-file.

Eboks is a private company that is partially and indirectly owned by the Danish state. The result is that a state controlled company now distributes and stores personal documents for more than a quarter of all Danes.

2.2 Case: Government PC-inspections

A working group at the Danish Board of Technology in April 2008 proposed that in order to access public web-pages, citizens would have to let the state run special software on their computers to let the state verify that the level of security was acceptable.

When IT-Pol pointed out the very obvious implication for the privacy of the citizens, the board argued that citizens already trust vendors of operating systems, middleware (e.g. Java), etc.

2.3 Why this is the wrong approach

Many of us are perfectly able to protect our own private data. The members of IT-Pol might be better at doing this than most Danes. But we believe most Danes would prefer to be responsible for their own private data. We do not think that the state is particularly competent in handling personal information.

Many Danes could need some help in handling personal data, but the state is not suited to provide that help for the following reasons.

- It will be a centralized solution. When it fails, it will have very serious consequences.
- Because of the many relations between state and citizen, the state is particularly susceptible to compromise privacy by function creep.
- The state has frequently demonstrated that it has an interest in monitoring its citizens, for example the recent extensive data retention legislation.
- When personal information is handled by the state, it means that we, as citizens, have no choice in who we entrust our personal information to. Therefore, we really loose control of our own data. We might trust Apple, Ubuntu (Canonical), Sun, or Microsoft to run the software on our computers, we might trust Google, Yahoo, Facebook, Wikipedia, etc. with our online activities, but that is our choice and if we feel that they abuse our trust, we can replace any software or service.
- When solutions are being forced on citizens, it can harm the relationship between the state and its citizens.

For citizens that can not, or do not want to, take care of personal data security there is no need to leave it to the state. Citizens should be free to appoint any proxy to do it. It could be their bank, their trade union, church, a family member, Google, etc.

3 Anonymity

We believe that we have the right to communicate with each other in privacy.

Anonymity is not an objective in itself and it has some drawbacks.

When engaging in public debates, we present ourself. We want other people to be able to contact us and we get credibility from our past work.

But we also understand that we are privileged. There are people that can not always be expected to let their online statements be linked to their private lives: whistle-blowers, victims of abuse, etc.

Many of us also use the Internet for tasks that are private. As a result of state surveillance and private interests, many tasks that we used to do in our private homes are now done one the Internet. For example, before the Internet it was not a secret which newspapers we were subscribing to, which books we were buying or lending, who we sending letters to, which goods we bought. But it was also not registered in centralized databases.

Now the state mandated data retention registers every website we visit and everyone we email with. Before the Internet, we would take the encyclopedia from the bookcase and look up anything and nobody would know what we were researching. Now we might Google it, and Google will register our search and link it with our Google email correspondence, or we could look it up in an online encyclopaedia, in which case the encyclopaedia would log which entries we read; and probably something like Google Analytics or Woopra would also log each individual lookup and link it to other traces we have left on the Internet.

The only realistic way of regaining some of our lost privacy is to use anonymity when we want to protect our privacy.

4 Polippix

The Polippix project is an effort to use technology to help people regain some of the rights and possibilities that have eroded either because of technology or by technology. The right to privacy is a very important example. Others, not discussed in this paper, are fair use (copyright) and the right to tinker (restricted by the Infosoc directive).

The primary expression of Polippix is a live-cd, that can be booted on most computers, and gives the user access to technologies used in Polippix.

4.1 Polippix Privacy Objectives

Polippix has gotten a lot of coverage as a tool to counter excessive Danish and European surveillance and data retention. This is deserved. The September 15, 2007 introduction of the Danish data retention is an important event, marking the day from which almost every Danish citizen came under daily observation without being under suspicion for any crime.

But there are many other threats to our online privacy, which are not marked by a particular day or year. The objective of the Polippix project is to protect users against all violations of online privacy.

From a technical point of view it does not make much of a difference whether Big Brother is the national police, a search engine company, an employer, a family member, a foreign country, or organized crime. These Big Brother candidates do not act independently. Personal data is traded between private companies, police exchange personal data across borders, national states can force private companies operating locally to release personal data on their citizens. A good example of this is the 2007 Danish data retention laws. Personal data is collected on request by the state, but is collected and stored by ISP's, wireless hotspot owners, hotels, housing communities, etc. This means that it is not just a matter of trusting the national police and intelligence with our private data, we also have to trust the personal integrity and technical competence of hotel owners, ISP's, etc.

It also does not matter why a Polippix user would want to keep Big Brother out of her private life.

- She could be doing something wrong.
- The mere collection of private data could violate her privacy.
- She could fear that her personal data could be abused.
- She could lack trust in legal and technical systems that should keep her private data confidential. I.e. Big Brother could be incompetent.
- She could lack trust in the people handling her data.
- She could have a need to assure others that the information she received from them would remain confidential. For example she could be a journalist communicating with confidential sources.

We therefore need a tool that will protect us against all threats to our private online life.

4.2 Privacy Technology in Polippix

Polippix is based on Linux and other free software. It is a live-cd based on the Kubuntu distribution. That allows users to try the Polippix software without installing software on their computers. It also prevents private information from being stored on hard-disks when using Polippix.

Some of the Polippix software relevant for privacy are:

- TOR (The Onion Routing) is a system enabling users to communicate anonymously on the Internet by routing data traffic though a few nodes randomly selected out of hundreds of thousands of TOR nodes. This does put a limit on the bandwidth and latency of the network.
- macchanger is a program that Polippix uses to change all network hardware MAC addresses at boot-time. This makes it impossible to link data traffic on local area networks to the computer on the network. E.g. when a laptop running Polippix is used on an open wireless network, data traffic cannot be linked to the laptop.

- Twinkle, SIP/ZRTP phone. Twinkle is an IP-phone using the SIP protocol. TOR is currently not able to handle very time-critical application like phone conversations, so privacy must be ensured by other means. Twinkle can use the ZRTP protocol for encryption of the conversation. This prevents eavesdropping, but not logging of participants in phone calls. It also does not provide anonymity, although anonymity is less important for phone calls because recognition of human voice also compromises anonymity.

  But when Polippix/Twinkle with macchanger is used on, for example, open WiFi access-points, registration of participants can be prevented.

  Even for IP-to-PSTN calls some degree of anonymity can be achieved. In PSTN the tracking of phone calls are based on the billing system. Because the price of phone calls to PSTN land-lines have dropped dramatically, it is possible to sponsor free phone calls for every user. I.e., the originator of every phone call is the sponsor, although the phone call could have been made from any of the distributed or downloaded CD's.

- GnuPG, bcrypt, etc are systems that can be used to encrypt data.

- wipe can securely erase harddisk or files on harddisks. Useful when selling a computer, handing it in for repair or returning it to an employer.

- jhead is a tool that can clean jpeg images from tags identifying the camera. We plan to add tools that can remove unwanted extra information from text documents, such as authors, editing history, older versions, etc.

- Etherape and driftnet: Etherape is a graphical network monitor that dynamically displays Internet connections. driftnet displays all images passing through a computer. We include these programs, because they illustrate how little privacy we have if we do not take measures to protect it.

Lessons Learned from the Polippix Project

The reception of Polippix outside our own environment has been overwhelming. 13,000 physical CD's were distributed to the members of trade union PROSA, more than 35,000 CD images were downloaded from our homepage and mirrors in a week, after that we lost track of downloads. Polippix has been covered on every major TV- and radio channel and all national newspapers.

The publics view on privacy and surveillance

In our contact with politicians, media, and even scientists, we have often encountered talking points that express that the public has accepted the invasion of privacy, that Big Brother is now a good thing, and that young people do not want privacy.

We disagree. We got in contact with many Danes after the release of Polippix. On September 15, 2007 when the data surveillance was introduced in Denmark, we took to the streets of Copenhagen, asking random people questions that reflected the effect of the introduced surveillance. The question (in english translation) included:

- Do you watch porn on the net? What kind?
- Are you a member of a political party or a religious society? Which?
- Do you eat pork when travelling on airplanes?
- Do you have regular contact with communists, xenophobes, or muslims?
- Who are the last 5 persons you phoned?
- What is your sexual orientation?
- How much do you earn per year?
- Do you consider your answers confidential? On a scale from 1-10, how much much do you trust us with your answers? The police?
- Can we publicize your answers?
- Do you want to give us your name and address to enter a draw for two bottles of wine?

From this we learned which parts of their lives, people wanted to keep private and it led to very interesting discussions about privacy.

- Many people actually do want privacy. That is why so many downloaded Polippix. They did not accept Big Brother. But some had accepted their fate of no privacy, because they did not know they had a way of avoiding it.
- There is an enormous variation in which parts of their lives, people want to keep private. For example, some were very frank about their sexuality, but would not reveal their salary, while others would not tell which organizations and societies, they were a member of.
- Most of the randomly selected people were not at all aware of the extent of the newly introduced surveillance. And after they were made aware of it, most of them did not accept it, or at least did not accept substantial parts of it.
- Younger people did seem more willing to expose themselves on the Internet. But they were also conscious about making the choice about what to expose.
- Even people that were not worried about the decrease in privacy were changing their behaviuor because of the surveillance, even if they were not doing anything illegal.

Community support

There is an overwhelming opposition to the data retention and other surveillance introduced by the state among IT-professionals in Denmark. It is our impression that this is caused by an interest in privacy, but also because most IT-professionals actually know and understand

exactly what is going on, realize the enormous implications for privacy, know that the measures will not help fight terrorism, and can seriously cripple the Internet as we know it.

Free Software is particularly well suited for the objectives of the Polippix project, because we need to use software technology to counter the technology of states, private corporations, etc. That can only work if we base it on software that can be used and developed independently. This is guaranteed by the four freedoms of Free Software as defined by the Free Software Foundation. Freedom to:

run software for any purpose even to counter government surveillance.

If we had to use non-free software we would have needed permission from every manufacturer of software used on Polippix. Considering that the Danish minister of justice has publicly criticized Polippix and that Polippix is now being used in some countries with a history of less democracy and respect for privacy, we doubt that we would have gotten the necessary permissions.

study how the program works, and adapt it to your needs Polippix users need to be able to verify that there are no back-doors.

redistribute copies so you can help your neighbour We needed to distribute tens of thousands Polippix CD'es and CD images. We want peer-to-peer distribution for anonymity. Any restriction on redistribution would have been fatal to the project.

We want Polippix users to be able to redistribute Polippix. This is the point of the CD/USB-memory replication schemes we are currently developing. If Polippix users could not freely redistribute Polippix then IT-Pol would be a bottleneck and a single point of failure for Polippix.

improve the program, and release your improvements to the public so that the whole community benefits

- That makes is possible to develop Polippix using existing Free Software projects.
- This ensures that Polippix cannot be easily stopped.

Conclusion

Polippix has helped create an informed debate about privacy.

Although most of the software on the Polippix CD originates from existing projects, getting a physical CD that circumvents the surveillance has been an eye-opener for many Danish citizens. It demonstrates that we give up privacy for practically nothing.

Although only a small part of the population uses Polippix or similar techniques, getting Polippix out to tens of thousands of Danes demonstrates that protecting your privacy is a very real concern for others than geeks and hard-core criminals.