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

Deliverable 3.3 Proposal Report

Final version April 2008

Start date of Activity: 1 February 2006 Duration: 28 month

Authors:
Maren Raguse, Owe Langfeldt, and Marit Hansen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

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**

Executive Summary

The use of Privacy Enhancing Technologies (PETs) as part of security technologies and security measures has not been discussed on a large scale and research in this field is scarce. The following measures and aims are discussed under the term PET. They are to be pursued in enhancing the data subject's privacy:

- Data minimization, including unlinkability, anonymity and pseudonymity
- Safeguards for personal data
- Control by the user
- Transparency of the system
- Audits and checks

PETs can lower the privacy impact of use of security technology by providing a least intrusive measure of fundamental right restriction and increase the possibility of proportionate use.

Since the level of privacy impact of security technology use is determined by

- the technical features of the technology,
- the general legal provisions allowing its use,
- and the actual use in a specific investigation,

looking only at technical features of security technologies is not sufficient. To enhance privacy, the following dimensions must be taken into account: hardware, data processing and organisational means. Privacy enhancing measures with regards to security technologies therefore embrace a technical, legal and organisational dimension.

This report maps known PETs to the basic technologies identified in D2.2 'Overview of Security Technologies'[1] as well as the general privacy principles derived in D3.2 'Legal Evaluation Report'[2]. While it is technically possible to apply all known PETs to security technologies, some of them contradict the underlying aim of law enforcement and criminal investigations (Chapter 2). This conclusion, however, does not exempt developers of security technologies from closely scrutinizing applicability of PETs to their research as implementation of PETs generally is also in the interest of the technologies' users (law enforcement authorities).

---

[1] PRISE Deliverable 2.2 Overview of Security Technologies

[2] PRISE Deliverable 3.2 Legal Evaluation Report

Key design proposals which ought to be taken into account in the design of security technologies and means span technical questions of IT-security measures, legal aspects regarding the introduction of provisions protecting a core sphere of privacy as well as the mandatory obligation to introduce a Data Management Process for FP7 security research.

Product and process related aspects introduced in this Report will be revisited and elaborated in the PRISE Criteria Report[3].

[3] PRISE Deliverable 6.2 Criteria for privacy enhancing security technologies

Chapter 1 Introduction

This Proposal Report will discuss options for privacy enhancing design of security technologies. The approach will cover the following three dimensions: technical features, legal framework and organisational embedding of a process to assure privacy compliance in research and development.

This report is going to present proposals in organisational, technical and legal dimensions with respect to privacy compliant security technologies and research thereof. The Proposal Report will describe which measures can and should be taken to ensure privacy enhancing design of security technologies and how to introduce considerations of privacy compliance and enhancement into the existing organisational processes in research and development.

The Proposal Report is directed at researchers who consider submitting a FP 7 proposal on security research as well as at such researchers already conducting security research funded by the European Commission. Proposals for FP 7 funding will have to pass an Ethics Review and the European Commission has stressed that proposals and ongoing research which do not achieve ethical compliance will not receive funding.[4] Early considerations of ethical and legal implications of a proposed project are therefore essential for researchers. In the context of security research a focus of ethical considerations do specifically lie on privacy implications of planned research and its future applications.

Furthermore, this report is directed at the European Commission's ethic review team, elaborating considerations for the ethical evaluation of proposals with regards to their privacy implications.

Finally, this report is directed at politicians forming the legal requirements for the application of security technologies. Even if these technologies are developed in a way that enables privacy enhancing use, the protection of human rights can only prevail if legal statutes allow the use of privacy enhancing security technologies or even regulate an obligation for use of privacy enhancing security technologies.

[4] 'Getting through ethics review' at http://cordis.europa.eu/fp7/ethics_en.html.

Chapter 2 Privacy Enhancing Design of Security Technologies

The call for privacy enhancing design of security technologies might seem as a contradictory postulation at first glance. Privacy enhancing technologies (PETs) so far have been defined as a coherent system of *information and communications technology measures* that

- protect privacy by eliminating or reducing personal data;
- or controlling access to all or parts of personal identifiable data according to policies and rules,
- all without losing the functionality of the data system.[5]

The Dutch health sector was one of the first to adopt PETs[6] but meanwhile their use has been expanded to other areas of application.[7] The European Commission endorses the use of PETs. It explicitly states that by means of PETs important public interests such as public security or the fight against crime could be better served as PETs are a tool to ensure that the law is respected and not breached.[9] So far, however, PETs have not been used in the context of security technologies on a large scale. The EC Data Protection Directive[10] includes an exception from the restrictions imposed on data processing if the processing is done for purposes of national security or policing. But as discussed in the Criteria Report[11], the principle of proportionality is still applicable here. PETs can, by lowering the privacy impact of security technologies, provide for a least intrusive mean and increase the possibility of proportionate use. Therefore, calling for privacy enhancing design of such technologies is not contradictory. It is perfectly justified, as the use of PETs might make measures proportional that without them would not be so. These measues could not be used without the implementation of PETs.

Previous research on PETs has not focused on an integrated approach focusing on the hardware side as well as on the software and data processing side of technologies. PET research usually is focused on partial questions. However, to enhance privacy, the dimensions hardware, data processing as well as organisational means must also be taken into account, not least because they are interlinked. What is needed is a holistic approach which still is lacking. The PRISE Project fills this gap and discusses societal, organisational, technical and legal aspects of privacy enhancing security technology design.[12] A second problem is that the research so far does not address security technologies as a context in which to use PETs. Such

---

5 Borking/Raab 2001

6 For a general overview of the topic, see the white book issued by the Dutch Data Protection Authority (2004)

7 See Dutch Data Protection Authority 2004: 8

9 See COM(2007) 228

10 Directive 95/46/EC, see D3.2 for a longer discussion

11 See PRISE Deliverable 6.2 Criteria for privacy enhancing security technologies.

12 In this deliverable as well as in D 6.2 Criteria for privacy enhancing security technologies.

technologies are not an obvious area of application for PETs, but nevertheless their application is possible and desirable.

Applying PETs in the context of security technologies is different from the context the use of PETs has been discussed in previously. If an individual is participating in business transactions or the provisioning of a service – even one offered for free – the relation between the individual receiving the good or service and the entity offering this product or service is governed by private law. The decision to receive or buy a service or good lies entirely with the customer. If the seller (or service provider) does not offer conditions the interested individual is willing to accept, he may simply choose not to do so and look for an alternative vendor or provider. The relation between the two is in general equal, even though a vendor with dominant market power or a service provider offering a niche service may be difficult to avoid by using a competing company or service provider. In this case the decision left may only be to agree to the conditions offered or to not buy or receive the product or service.[13]

In the context or law enforcement and crime prevention public law (criminal law) is applicable. The relation between the citizen and the government as participating entities is not equal but the citizen is in a subordinated position. For a citizen it is not a matter of choice whether or not to become subject of a criminal investigation or security technology use. The rights and obligations of citizens during a criminal investigation are regulated in Criminal Procedure Acts and are linked to specific roles like witness, victim, or defendant. Depending on the procedural role, certain privileges may apply as for example the privilege of a witness or defendant to decline to answer questions (and thus not to reveal specific information himself).

[13] On the concept of policy negotiation replacing the 'take it or leave it' approach see Leenes/Hansen/Schallaböck 2007: 12

The following figure presents the described difference:

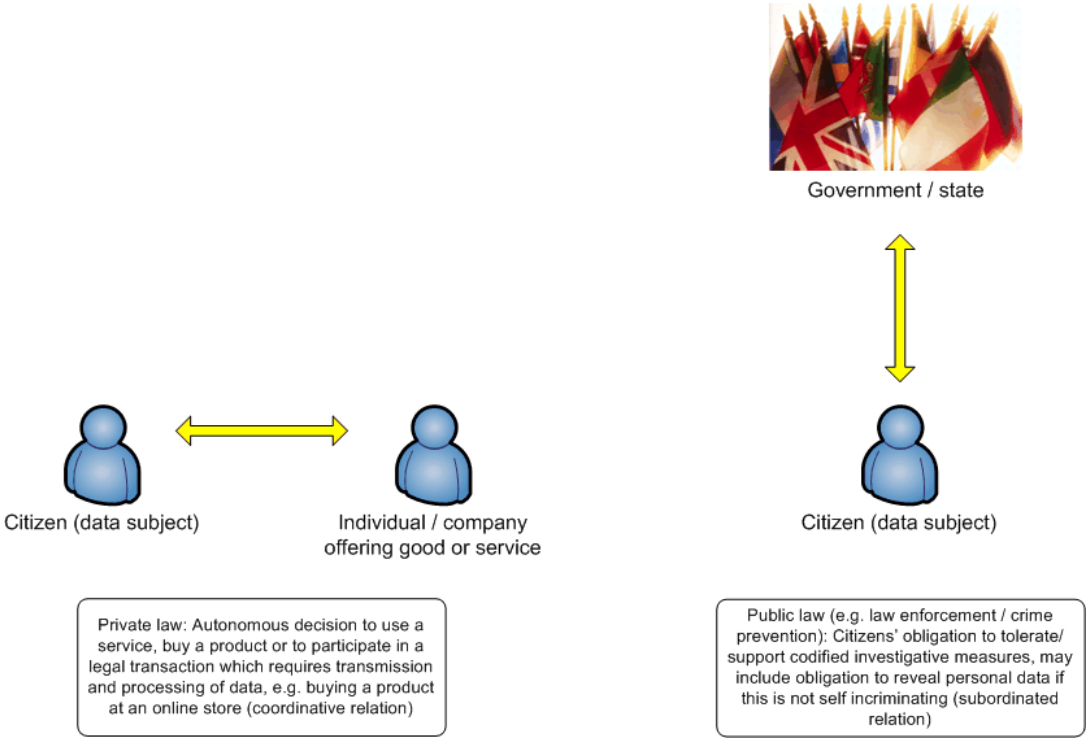

Figure 1: Difference Private and Public Law (Criminal Law) and citizens' choice

It is thus necessary to further analyse if and where in the context of security technologies the call for PETs is valid. The Commission in COM(2007) 228 considers the benefits of PETs and points at their purpose of making ‘breaches of the data protection rules and violations of individual’s rights […] technically more difficult’.

The following goals are to be pursued in enhancing the data subject’s privacy:

- Data minimization, including unlinkability, anonymity and pseudonymity
- Safeguards for personal data, e.g. encoding of rules and policies
- Control by the user
- Transparency of the system
- Audit and checks

Where is the link between the goals stated above and the privacy principles[14] identified in the earlier work of PRISE?[15] PETs serve as technical means to enforce them. Legitimacy can be provided for by technologies for control by the user which help to meet the criterion of consent. Purpose binding can be enforced via unlinkability and supporting measures like control of the user and pseudonymity, as these make linking data from different sources more difficult. Proportionality can be ensured by the use of technologies that minimise the amount of data collected as well as by anonymization. The appropriate quality of the data can be provided for by access and control rights for the users. Transparency and security of the data translate directly to their corresponding PETs. Sticky Policies[16] technically enforce purpose binding and thus ensure legitimacy. The term "sticky policies" describes privacy policies which are linked with personal data. The privacy policies are passed on with the data and enforce the rules how the data may be processed even after they have been disclosed and thereby have left the data subject's control. Sticky Data Tracks can serve as a means to deter unauthorised access and make audits of data processing possible, thereby providing for security of the data and transparency. The term "sticky data track" describes a history function of all processing carried out regarding specific data. It stores when which personal data have been disclosed to whom and under which conditions. This history is passed on with the data and can be reported back to an application used by the data subject.[17]
The four basic technologies identified in the Technology Report[18] can also be related to PETs. The following table shows which PETs can be used in the context of the identified basic technologies. It can only provide for a very rough overview; the connection between different PETs and the basic technologies will be elaborated below in the chapters dealing with each of the former.

Basic technology	*Associated PETs*
Sensor technology	Data minimization, transparency
Communication technology	Transparency, security of personal data
Data storage	Anonymity, pseudonymity, access and control rights, security of personal data, unlinkability, data minimization, sticky policies, sticky data tracks
Analysis and decision-making	Anonymity, pseudonymity, data minimization, transparency, sticky policies, sticky data tracks

[14] These principles are: legitimacy, purpose binding, proportionality, transparency, quality of the data, security of the data.

[15] PRISE Deliverable 3.2 Legal Evaluation Report, p. 21

[16] The concept of sticky policies was introduced by Karjoth/Hunter 2002 and elaborated by Cassa Mont / Pearson/Bramhall 2003. See also Hansen 2008.

[17] See research carried out by the PRIME project.

[18] PRISE Deliverable 2.2 Overview of Security Technologies

These privacy enhancing measures embrace a technical, legal and organisational dimension. After giving a general introduction to the privacy enhancing measures mentioned above, this report will describe in more detail the technical, legal and organisational dimension of privacy enhancing design in the context of security technologies.

The following figure presents how the different dimensions of privacy enhancing measures are connected to each other. Note that not all of the aims enumerated above are included in it.[19]

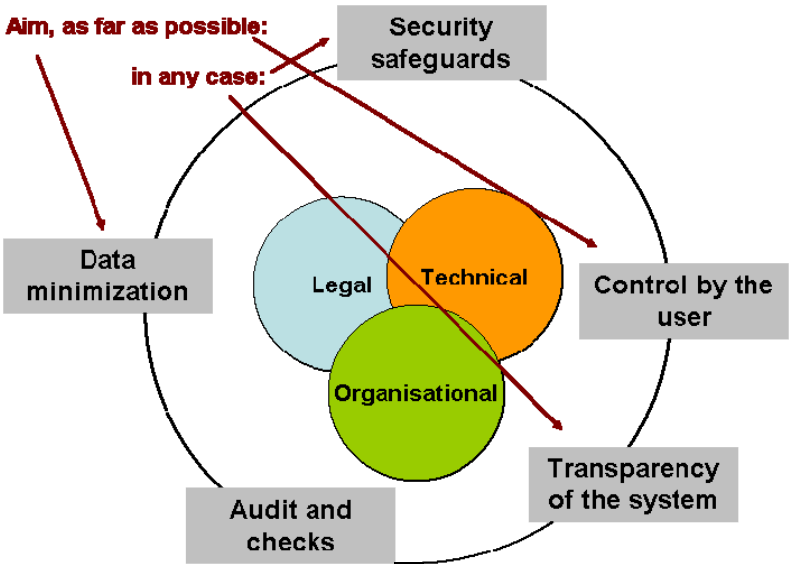

Figure 2: Dimensions of privacy enhancing measures (Köhntopp, 2001)

Not all of these measures seem to be applicable for security technologies which aim at detecting conspiracies to commit criminal offences at an early stage, restore and maintain public order and enable and support the investigation of criminal offences. Control by the user as well as transparency don't seem to fit a covert investigation. This chapter will – for each of the PETs enumerated above – give a short definition before turning to existing technical or organisational measures to implement them in other contexts. In a third step some thoughts on how to implement these in the context of security technologies will be presented. This three-step structure will be replicated for each of the PETs.

2.1 Data minimization

The term data minimization refers to minimizing the amount of personal data being processed in an IT system. Data minimization means not collecting data that are not necessary for the envisioned purpose and/or anonymization and pseudonymization of personal data as means of data avoidance. Traditionally, system developers have thought the amount of personal data

[19] Still, it may be argued that anonymization can be seen as a part of data minimization as it reduces the amount of personal data being stored. A similar argument may be made for pseudonymization. Unlinkability is harder to subsume under these headings, but it is instrumental in ensuring user control and transparency since it prevents function creep.

necessary to be an external condition imposed by the purpose of data processing and thus not alterable by design. However, this turned out not to be true; it is possible to reduce the amount of personal data being used for a specific purpose without impinging on the system's functionality[20]. Data minimization also covers limitation of possible use of data as well as technically ensuring purpose bound use.

Concrete ways to implement data minimization would include questioning every recording and processing of personal data – preferably already when defining a product's functionality and developing it[22] – to see whether it is really necessary for the specific purpose. Reducing the amount of data collected is a very difficult task in existing systems and thus data minimization should be considered at the earliest time possible. Technological means to implement data minimization are mainly anonymization and pseudonymization, often based on cryptography.[23]

Data minimization is especially hard to implement in the context of security technologies, since many new security technologies rely heavily on the collection of lots of data, e.g. face-recognition technologies. One of the practical implications of the rapidly expanding use of video surveillance in public spaces in some countries has been that there is simply too much data. This has led to the development of 'pattern recognition' type of intelligent cameras, that only starts recording, once a suspicious or unusual moving pattern appears, of if a recognizable person, vehicle or asset is in focus. Besides leading to data minimization, it also relieves a lot of innocent people from having their moving patterns disclosed. Ideally, data minimization should be implemented on the level of sensor technology – data not collected is protected the best. But since many new technologies rely on indiscriminate collection of data, this may prove to be hard. Data mining is an important example of a technology for analysis and decision-making. Constantly evaluating the algorithms used for mining and discarding attributes which do not improve the quality of results[24] can help to minimise the amount of data processed.[25] In the context of storage technologies deleting data as early as possible and as soon as mandatory is imperative.

2.1.1 Anonymity

A definition of anonymity is given by Hansen and Pfitzmann: Anonymity is the state of not being identifiable[26] within a set of subjects, the anonymity set. To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes.[27] Anonymity is not framed as an absolute term here; one may have more or less anonymity. The assessment of the quantity of anonymity is based on the efforts an attacker has to make to establish the link between a subject and the respective data.[28] Also a differentiation

---

[20] Working Group on "Data Protection in Telecommunications" of the Committee on "Technical and organisational aspects of data protection" of the German Federal and State Data Protection Commissioners 1997.

[22] See below, Chapter 3.3.1

[23] Hansen 2003: 17

[24] And do hence not enable data quality as one of the principles laid down in Directive 95/46.

[25] See Meints/Möller 2007

[26] For an in-depth analysis of the element ‚identified or identifiable natural person' (Art. 2 lit. a Directive 95/46/EC) see Working Party 2007: 12

[27] Hansen/Pfitzmann 2007, especially 7-10

[28] See Hansen/Pfitzmann 2007: 8

is needed between the anonymity of the system as a whole and that of individuals within it, as the "usual suspects" might show patterns that differentiate them from the rest of the system.[29]

With regards to storing and processing of data, anonymity can be ensured by providing the possibility of anonymous use of services, thus not collecting data in the first place. Anonymous calling cards are a classic example. It has to be noted that anonymity does not imply that there is no way to prevent unauthorised use – just as shown by calling cards, authorisation is possible without identification.[30] If the collection of personal data is inevitable, it has to be checked whether storing them for a longer period is necessary. If the data is only used for statistical purposes, personal identifiability is not needed and the data can be anonymised. This is also an example of how technical (the actual anonymisation) and organisational (checking whether personal data is still needed) measures are interlinked. Concerning transmission technologies, anonymity can be provided for via measures such as onion routing[31], mixes[32], or DC-Net.[33] The effectiveness of these measures can be enhanced by the adding of dummy traffic.[34]

How can these measures be applied to security technologies? In the context of technologies for different kinds of access control, the distinction between identification, authentication and authorisation has to be observed.[35] Criminal investigations aim at identifying the perpetrator of a crime. Only if evidence establishes causality between a prohibited act and a natural person, this person can be held responsible for his or her acts. So lifting anonymity of a suspect is an essential part of law enforcement authorities' tasks. This is however only necessary for the suspect and not for all other individuals who are subject to investigative or preventive measures but against whom no concrete suspicion can be established. Yet, as soon as information held by an individual seems relevant for an investigation and personal interrogation is considered necessary, this person has to be identified in order to carry out the interrogation. In computer-aided searches the identities of many innocent persons are revealed as further investigation is deemed necessary if an individual matches the before defined profile. However, approaches to privacy preserving data mining have been presented.[36] Revoking the anonymity of a suspect based only on a concrete suspicion and a court warrant should be considered in this context. The participatory interview-meetings carried out in 6 European countries indicate that security measures are more acceptable to a majority of participants if a court order and strict control measures are required and in place.[37]

---

[29] Clauß/Schiffner 2006

[30] Basically, access controls (be it to rooms, services etc.) are about three things: Identification – "who are you?", authentication – "prove that you are who you claim to be" and authorisation – "what are you allowed to do?". However, not all three aspects are necessary in every context. Schneier provides an example: That of a substitution facility for heavy drug addicts which uses ID-Cards that do not have a name, but only a picture on them. This provides authentication and authorisation. Identification is neither wanted nor needed here, see Schneier 2003: 181-206

[31] See http://www.onion-router.net/ and http://tor.eff.org/, see also Hansen et al. 2007: 162 and Chaum 1981

[32] Hansen et al. 2007: 158-162

[33] Chaum 1988

[34] Pfitzmann/Pfitzmann/Waidner 1991

[35] Hansen/Pfitzmann 2007, especially 7-10.

[36] See Meints/Möller 2007

[37] See PRISE Deliverable 5.8 Synthesis Report Interview Meetings

A small deviation from the standard three-step procedure is justified here to discuss the implications of the EC directive on data retention.[38] This directive requires operators of publicly usable telecommunications services, i.e. (mobile) phone companies and internet and e-mail providers, to store traffic data for a period of 6 to 24 months.[39] The data to be stored include who was in contact with whom at what point of time. These provisions essentially make anonymous use of phone networks impossible. This regulation seems contradictory to the thoughts presented here – if the directive mandates the retention of personally identifiable traffic data, there seems to be no point in thinking about anonymity anymore. However, this is not the case, as the directive applies only to publicly usable networks and only on the access level and not the content level.[40] In PRISE, the focus is on privacy enhancing design of technologies which are to be used *within* corporations or institutions, and thus outside the applicability of the directive. Transmission technologies like RFID are also beyond the directive's scope.

However, the directive on data retention can be seen as a postulation of the EU institutions' position towards anonymity in public networks. Article 5 clearly states the aim to enable tracing and identifying the source of a communication. Whether the directive is applicable to anonymization services is doubtful, as these are no 'providers of publicly available electronic communications services or of a public communications network' (Article 3 (1) Directive 2006/24/EC). It can be concluded that the EU institutions consider anonymous access to communication to impair law enforcement and criminal investigations. As described above, a central element of criminal investigations is to narrow down and finally identify the suspect of a (planned) criminal act. This fact should, however, not be turned into a general obligation to always be identifiable whenever engaging in receiving a service, buying a product or other actions which may be of relevance for a later criminal investigation. Such a claim would violate the presumption of innocence and completely defeat the right to informational self-determination.

It can be concluded that the right to anonymous use of internet and telecommunication services has been restricted on the access level.

2.1.2 Pseudonymity

A further approach to enforce data minimization is pseudonymity. Pseudonymity refers to the use of pseudonyms as identifiers for persons or other entities.[41] A pseudonym is a name other than one of the subject's real names.[42] A pseudonym need not be secret – the difficulty of linking a pseudonym with the real identity can vary. Roughly, three classes of pseudonyms can be described:

- Public pseudonym – the connection between a person and his/her pseudonym is publicly known. An example would be a telephone number listed in a phone directory together with its owner.

---

[38] Directive 2006/24/EC

[39] Determining the precise duration within this frame is left to the member states.

[40] See Art. 3 (2) of 2006/24/EC

[41] For this section see Hansen/Pfitzmann 2007: 19-26 and Hansen et al. 2007: 165-167

[42] In the context of natural persons, the real name usually is the legal name.

- Initially non-public pseudonym – the link between a pseudonym and its owner is only known to certain parties in the beginning. An example would be a phone number not listed in a public directory, with the link initially only known by the number's owner and the phone company.
- Initially unlinked pseudonym – the link between the pseudonym is (at least initially) not known to anybody, maybe excepting the owner himself/herself. An example would be biometric information not stored in central databases.

In the first case linking obviously is very easy. The second class of pseudonyms offers a wide range. Some of the pseudonyms grouped in it become – at least after they have been used for a certain time – easily linkable to their holders, such as social security numbers, especially when they are also used for other tasks than the administration of social services.[43] Others may be harder to link.[44] An example would be the work of identity brokers. These authenticate digital pseudonyms by connecting them to a real person and then issuing a digitally signed statement indicating that the brokers knows the person's true identity. This information is only divulged in certain, well-defined situations (e.g. on court order in the case of criminal investigations).[45] This may serve to ensure accountability in spite of not knowing the subject's true identity. Similar techniques might be used in applications such as privacy preserving data mining[46] where the identity of persons is only revealed on a concrete suspicion. The third class is the hardest to link. To pick up the example mentioned above, biometric information can be used to establish such pseudonymity. A more elaborated version of the example would be the template of a fingerprint stored on a smartcard. To authenticate, the holder has his finger scanned, the image is transformed into a template which is then compared to the data on the card.[47] As long as this data is not stored, this may provide authentication without revealing the person's identity.

PETs providing pseudonymity include identity and privacy management systems[48], i.e. systems that create pseudonyms and only disclose information to the extent needed. They allow users to exercise more control over their personal data. The term privacy management refers to systems that apply privacy rules to personal data, e.g. "organisation X may use this data only for purpose Y and may not share it, except with organisation Z for purpose W". Examples would be P3P[49] for internet users or EPAL[50] for the use in corporations or institutions. Identity management systems help to generate and manage different identities, so the user controls what data about himself he wants to reveal to a service provider or other party, thereby further preventing the linking of data.[51] It is also possible to transfer credentials

---

[43] An example of such use would be the Austrian education monitoring system, which uses the social security number as a unique identifier, see: http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=19898ulr

[44] An example are the sector specific identifier as used in the Austrian Bürgerkarte. See overview at http://www.fidis.net/resources/deliverables/hightechid/int-d36000/doc/31/

[45] On digital identities in general, see Hansen/Meints 2006 and Hansen/Meissner 2007

[46] Hansen/Pfitzmann 2007

[47] See Hansen et al. 2007: 149

[48] For example the PRIME project, https://www.prime-project.eu/ see also Hansen et al. 2004.

[49] See http://www.w3.org/P3P/

[50] See https://www.datenschutzzentrum.de/adam/index.htm

[51] See for example the concept of an "identity protector" in Hes/Borking 2000

from one pseudonym to another without proving that the owner is the same.[52] The question of linkability will also be addressed in the next subchapter.

But can identity and privacy management system be used in the context of security technologies? Privacy management systems usually rely on control by the data subject, which for obvious reasons is not feasible in this context. But nevertheless mechanisms similar to identity management system might be used in the context of storing and analysing data. An example would be pseudonymising personal data which are to be used in computer-aided searches and only re-establishing the link to the person on the basis of a court order. This helps both to ensure proportionality and to prevent abuse of the data. As the use of different pseudonyms also hinders linking data from different databases, it also helps to prevent function creep and enforces purpose binding. Furthermore, role management and access management as a form of identity management is important to implement at law enforcement authorities to ensure authorized access to stored and processed data

2.1.3 Unlinkability

Unlinkability refers to the impossibility to judge whether a set of items of interest (IOI) is related or not, e.g. whether it is possible to link these items (which may be, inter alia, persons, messages or actions) within a specified system (which may, for example, be a customer database, but could also consist of different databases combined for data-mining). Just like anonymity, this term is not absolute. A system may provide for more or less unlinkability based on the efforts an attacker would have to make in order to link the data. To quote Hansen and Pfitzmann:

"Unlinkability of two or more items of interest […] from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not."[53]

Concrete examples of measures useful for ensuring a sufficient degree of unlinkability would include the use of different pseudonyms for different purposes. This would ensure unlinkability between databases (serving as an equivalent to data separation within an organisation). This can be facilitated by the use of identity management systems (see 2.1.2 above for a description). Unlinkability can also provide for a certain degree of anonymity.[54]

Relating unlinkability to the four basic technologies, its place is in storage technologies. Data stored has to be anonymised or pseudonymised[55] to ensure unlinkability between different databases. Unlinkability is crucial in enforcing purpose binding, one of the privacy principles identified in the Legal Evaluation Report [56]. It also helps to prevent function creep.

---

[52] See Chaum 1990 and Cemenisch/Lysyanskaya 2004

[53] Hansen/Pfitzmann 2007, p. 10, see fn. 27

[54] Hansen/Pfitzmann 2007, p. 25

[55] Obviously, different pseudonyms have to be used in the different databases, see Spiekermann/Cranor 2006: 25

[56] PRISE Deliverable 3.2 Legal Evaluation Report

2.2 Safeguarding personal data

Security of personal data, i.e. protection against unauthorised access, change or processing, also helps to preserve and enhance privacy by preventing unauthorised access to or processing or forwarding of the data. Measures for safeguarding personal data must be implemented on a technical as well as an organisational level. Standards for securing data against such threats are well established in the field of IT-security, which shares some goals with data protection. The main goals of IT-security are confidentiality, integrity and availability of data. The first two provide for a significant overlap with the privacy principles identified in the Legal Evaluation Report [57].

The most important standard here is ISO 27001[58] which describes guidelines on how to plan, build up and run an Information Security Management System (ISMS). However, it does not describe good practice workflows in detail. This is done for example in the baseline protection catalogues issued by the German Office for Information Security (BSI).[59] The Common Criteria, which are based on ISO 15408 and focus on products, are another important standard in this area.[60] Examples of measures stipulated include the encryption of transmission and storage of data as well as digital signatures. A role-management for the data processors ("who may know and do what?") is also necessary. Furthermore, security technologies to be used have to be protected against manipulation and should provide an easy to use interface.

These standards are applicable to security technologies without difficulty and no restriction applies. They are especially needed in the context of storage technologies to prevent unauthorised access to and processing of data.

2.3 Control by the user

Control by the user refers to the data subject having control over his/her personal data and being capable of deciding who shall have access to the data for what purposes. It also emphasises the need for consent on part of the data subject. This notion is part of the case law of the German Constitutional Court which established the "freedom of informational self-determination".[61] It also encompasses protection against profiling, as it implies control about the (un)linkability of data.[62] Similar to the section on transparency, a clarification of terms is needed here, as control of the user can refer both to the user of the technology and to the persons being subject to these technologies. User control in the context of security technology still is understood to mean control by the data subject.

Control of the user can be ensured via tools like P3P[63]. Privacy and identity management systems[64] can also provide for control of the user as they make linking data more difficult.[65] An

---

[57] PRISE Deliverable 3.2 Legal Evaluation Report

[58] See http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[59] See http://www.bsi.de/gshb/index.htm

[60] See http://www.bsi.de/cc/index.htm

[61] See BVerfGE 65,1, the so-called "census decision"

[62] Hansen et al. 2007: 7

[63] See http://www.w3.org/TR/P3P/

[64] See above 2.2 on pseudonymity and Hansen/Pfitzmann 2007: 27-31

[65] See also above 2.3 unlinkability

example of such a system would be the identity protector developed by J. J. Borking.[66] The "notice and consent"-approach can also be used to provide for control on part of the user.[67]

In the context of security technologies, this goal is at first glance hard to attain. In covert investigations, for example, control of the user (data subject) is obviously not wanted. In the context of other security technologies, it may be easier to implement, but still it remains hard. An example would be to offer the possibility of opting in. But then, a problem may arise if this opt-in undermines the effectiveness of a technology. From the point of view of the organisation using a technology, control of the user can be ensured via organisational measures like having a human checking and authorising actions to be taken by system. This can be seen as a kind of "notice and consent" and as an implementation of art. 15 of the Data Protection Directive,[68] which bans automated individual decisions. While during an ongoing investigation control of the user over

- being subject to security technology use and
- whether or not to reveal personal data

is limited, user control still takes a prominent role in procedural criminal law. If the type of investigation made notification during the ongoing investigation impossible, obligations to notify are usually in place for the time after the end of the investigation. This is to enable transparency and control by the user in the form of seeking judicial scrutiny of the investigation at question and measures used therein. Furthermore, the nemo tenetur principle[69] can be seen as a legal means to ensure control of the user (data subject) in the context of law enforcement. While the data subject can refuse to answer questions if an answer would be self-incriminating, exercising this right is only possible if the data subject is aware of being subject of a criminal investigation. Exercising this right is applicable mostly during interrogations. If a covert technology use is taking place, control of the user (data subject) again is not enforceable.

To safeguard the rights of the data subject access and control rights are necessary. These refer to the right of the data subject to access the stored data and have it corrected if it is incorrect. This is important because decisions made on the basis of incorrect data can have adverse consequences on individuals, e.g. entries on no-fly-lists. As the Commission points out in COM(2007) 228 final, 'the use of PETs should result in making breaches of certain data protection rules more difficult and/or helping to detect them'.

Measures to guarantee these rights include for example automated procedures that provide the data subject with access to the data stored about him/her and preferably also procedures to correct incorrect data. In the case of covert investigations, these are difficult to implement as doing so might endanger the officers who conduct the investigation. In such cases, an ombudsman or "citizen's attorney" has been suggested to provide relief. Such a person would

---

[66] See Hes/Borking 2000

[67] Spiekermann/Cranor 2007

[68] Directive 95/46/EC

[69] The right not to self-incriminate.

act as 3rd party that ensures that the rights of the data subject are respected, including challenging surveillance measures in court.[70] However, this is a purely organisational measure and only a second-best solution. Concerning technologies that do not rely on covert use, the usual notification and correction procedures can be used.[71]

2.4 Transparency of the system

Transparency means that the amount and kind of data collected and how it is processed (and/or linked to other data) is known to the data subject.[72] Transparency in the context of security technologies has two faces. One is transparency of the system towards its operator, e.g. a police agency. The other is transparency towards the subject of these technologies, i.e. the person the technology is used upon. The latter kind of transparency is especially important with respect to technologies involving the remote collection of data, such as RFID and CCTV.[73]

Transparency can be enhanced by measures that notify the data subject that data is being collected and processed. An organisational measure to ensure transparency is the "notice and consent"-approach[74] in which the user is notified about the company's or application's privacy policy, i.e. what data are collected, for what purposes are they used, how long are they stored and whom are they forwarded to, and then offers the choice of opting-in. All this obviously has to be done prior to data collection. Technical measures to ensure transparency would for example include light emitting diodes on cameras that light up when the camera is active. Similar to this, card readers can notify the data subject that data is being transferred. Signs indicating that a certain area is being supervised via CCTV are another classic example. Transparency is not only needed in the context of sensor and transmission technologies; analysis and decision-making technologies require transparency just as well. Here, however, it becomes more difficult to ensure transparency. Measures to be taken might include that the law enforcement authority notifies the data subject on the data processing and its methods. Transparency concerning the forwarding of data to other parties is also important in order to preserve unlinkability.

A fairly new topic of research is the concept of meta information attached inseparably to personal identifiable information (PII) similar to the way Digital Rights Management (DRM) is implemented in music files enforcing the rights of the copy rights owner. Two different approaches are discussed, both aiming at enforcing individuals' privacy rights.

Research conducted in the EU research project PRIME (Privacy and Identity Management for Europe)[75] elaborates the concept of *sticky policies*: 'Sticky policies are a way to cryptographically associate policies to encrypted (personal) data. These policies function as a gate keeper to the data. The data is only accessible when the stated policy is honoured'.[76] In the context of law enforcement and crime prevention applying this concept to all data available in

[70] Borchers 2007

[71] Their legal bases are art.12 of 95/46/EC and the correspondent regulations in the national privacy laws.

[72] On the need for Transparency Enhancing Tools (TETs) see Hildebrandt 2007

[73] For the first see Hansen et al. 2007: 156

[74] See Spiekermann/Cranor 2006 p.29-30

[75] Project website https://www.prime-project.eu/

[76] Leenes/Hansen/Schallaböck 2007: 12

police databases would aide the authorisation concept which should be expected to be implemented at every police station following basic IT-Security principles. The sticky policy could contain a rule similar to 'only officers with authorisation level X can access these data' and thus technically enforce authorized access. Furthermore, the sticky policy can enforce legitimacy and purpose bound processing of data by for example stating

- whether the PII may be transmitted to specific third parties, e.g. authorities of other Member States,
- whether the PII may be linked with data from other sources, e.g. to run a computer aided search or for means of profiling,
- whether the PII 'expired', meaning the retention period permissible by law is over and the data should already have been deleted.

A similar approach has been introduced with regards to the concept of *sticky data tracks*.[77] Sticky data tracks are a way to associate the access history or access log of PII to the personal data. This allows later scrutiny of who accessed the data at what point in time and can support internal controlling or supervision at law enforcement authorities as well as later judicial scrutiny during a trial.

These measures can be implemented in the context of security technologies. Sticky data tracks can be implemented to make audit trails. Sticky policies can also be implemented, but there is a downside to them. In the context of law enforcement they would require that all agencies involved use the same system for them or else they cannot access the data. Even though judicial and police cooperation is a growth area in European integration[78] such an approximation in the data processing system used by law enforcement agencies seems unlikely for the time being. Nevertheless, their use is to be considered when developing security technologies, as they can augment the data subjects' privacy considerably

The aim of transparency can be hard to meet in the context of security technologies, since e.g. covert investigations rely on the subject not knowing about them and thus the "notice and choice"-approach cannot be applied here. Also, even if an investigation is not covert, neither the suspect nor for example witnesses are entitled to know about every investigative step of the law enforcement authority, even if it is directed at them. Usually, the right to access the investigation file, possibly represented by an attorney, is in place. But on the other hand, knowledge about being or having been investigated is crucial to challenge investigations in court and thus for the rule of law. On these grounds, a certain level of transparency is needed even in security technologies – at least ex post. On the other hand, transparency is also needed towards the operators of the security technologies – they need to know what the technology is doing. Concerning technologies that do not rely on covert use, the fact that data is being processed or collected has to be made transparent. This can be done via the methods described

[77] This term has not been explicitly introduced by the researchers working on this concept, but describes the underlying approach concisely. See Grimm/Meissner 2007: 51-57

[78] Monar 2005

in the second paragraph.[79] Summarising this, it can be said that transparency is needed in all four basic technologies, although it may prove difficult to implement.

2.5 Audit and checks

Organisational and technical measures alone are not sufficient to ensure privacy enhancement of technologies. In addition, prior checking as well as regular checks by the responsible supervising data protection authority are necessary.

2.6 PETs research mapped to basic technologies

In the Technology Report[80] the PRISE project introduced an abstract model aiming to simplify a first assessment of frequently to be found privacy implications associated with the four basic technologies and a combination thereof. Security technologies consist of one or a combination of several of these identified basic technologies. The following figure[81] maps the basic technologies identified in PRISE to the correlating steps of data treatment:

[79] See the policy advice in Hansen et al. 2007: 210-212

[80] PRISE Deliverable 2.2 Overview of Security Technologies

[81] Taken from PRISE Deliverable 3.2 Legal EvaluationReport, p 32

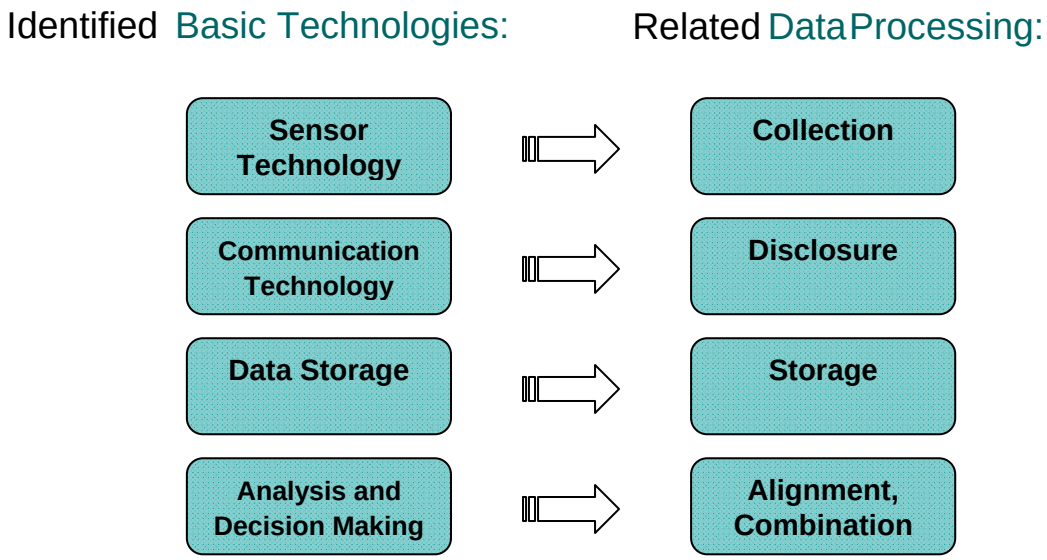

Figure 3: Identified Basic Technologies and related Data Treatment

Following this categorization, an overview will be presented of research on privacy enhancing technologies which can be mapped to the four basic technologies.

2.6.1 PETs and sensor technology

With regards to the basic technology corresponding the data treatment step of collection, research on privacy enhancement is comprehensive. For optical sensor technologies, CCTV is a prominent example. The development of intelligent CCTV-systems with algorithms for context-aware, behavioural risk analysis is a growing area of research. In this context IBM has conducted research on video privacy[82] and has released[83] a Digital Video Surveillance service which is described to allow real-time analysis of behaviour. The service, called 'S3' is described to *allow* automatic anonymization of non-suspicious video data.[84] S3 is reported to be used for video surveillance in the city of Chicago[85] and by 'several governments, law-enforcement agencies, airports and some businesses'[86]. The feature allowing anonymization is, however, not the default setting. Instead, according to Charles Palmer, chief technology officer of IBM Security and Privacy 'the entity doing the surveillance has to request that that feature be in place'.

---

[82] More information at http://domino.research.ibm.com/comm/research_projects.nsf/pages/s3.videoprivacy.html

[83] See press release at http://www-03.ibm.com/industries/government/doc/content/news/pressrelease/1904419109.html

[84] See Heise Online: 'IBM stellt intelligentes Video-Überwachungssystem vor', 8.11.2006. Available at http://www.heise.de/newsticker/meldung/80748 (in German)

[85] See Heise Online: ' Chicago setzt auf "intelligente Videoüberwachung" ', 27.9.2007. Available at http://www.heise.de/newsticker/meldung/96687 (in German)

[86] See ZDNet.co.uk: IBM surveillance could monitor borders', 7.11.2006. Available at http://news.zdnet.co.uk/security/0,1000000189,39284580,00.htm

More simple means of data minimization in the context of CCTV can be achieved by restricting the angle and zoom resolution of the camera.

A focus of privacy enhancing technologies research has been on the RFID technology. Approaches have for example been presented in form of a 'privacy checklist for privacy enhancing technology concepts for RFID'[87]. Sieker/Ladkin et al. present the following checklist for an analysis of privacy enhancement of RIFD:

The Privacy Enhancing Technology (PET) concept ...

a. enforces making sparing use of data?
b. makes privacy the default?
c. transfers control to citizens?
d. sends tags to a secure mode automatically?[1]
e. can prove that automatic activation of secure mode always works?
f. prevents eavesdropping of tag-reader-communication?
g. protects citizens from producer?
h. protects citizens from retailer?
i. protection includes in-store problem?
j. protects tag in secure mode against presence-spotting?
k. does not require citizens to take active protection measures?
l. does not interfere with active protection measures?[2]
m. avoids creation and use of central database(s)?
n. avoids creation and use of databases at all?[3]
o. enables functionality after point-of-sale in a secure way?[4]
p. can be achieved without changing RFID physical technology?
q. does not make tags much more expensive?
r. does not make tags more expensive?
s. does not introduce additional threats to privacy?
t. introduces additional benefits for privacy?
u. provides benefits for the retailer?

[1] unsafe tags are disabled forever („killed") automatically
[2] e.g. using blocker tags. Active protection measures are controversial but there should be no loss in privacy protection through interference with other privacy protection
[3] databases allowing to create associations between objects and people either directly or indirectly
[4] e.g. intelligent fridges or washing machines

Figure 4: Privacy Enhancing Technology concept for RFID

Other solutions discussed range from Faraday Cages, RFID sensor detectors, active jamming (or blocking) on the consumer side to manufacturer side solutions like 'kill command' features, the clipped tag[88] or smart RFID tags with a hash-lock.[89] These approaches aim at transparency, security of the data as well as control of the user.

It has to be noted that not all of the approaches presented for PETs in the context of RFID focus only on the sensor part of the RFID system. RFID comprises at least three of the basic technologies identified by the PRISE project: sensor, communication and storage technology.

[87] Sieker/Ladkin et al. 2005
[88] Moskowitz/Lauris et al. 2006
[89] For an overview see Karjoth 2006 and Rieback/Crispo 2005

2.6.2 PETs and communication technology

General approaches regarding privacy enhancement of the data treatment step of transmission cover encryption of the transmission, as well as anonymization of internet use. Communication technology as a basic technology in the context of the PRISE project is used for technologies enabling transmission of data. Applying a simplified version of the 7 layer OSI model[90], three layers can be identified which are required for a network communication process:

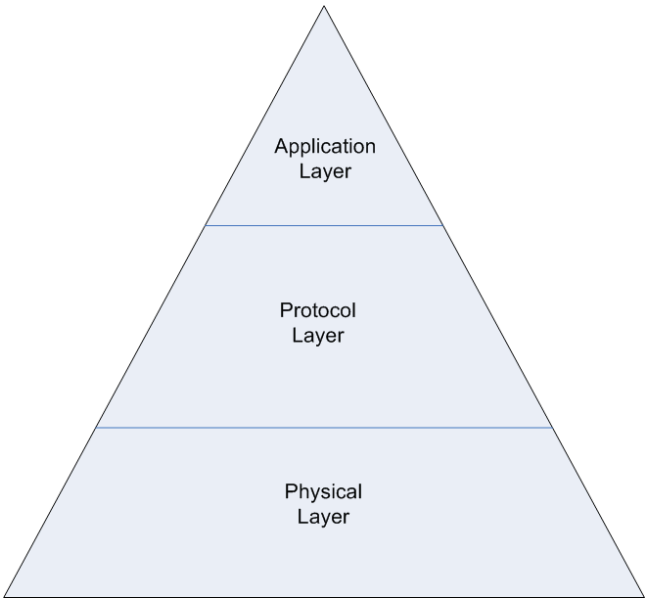

Figure 5: Simplified 3-Layer model for a network communication process

The PRISE project, when using the term communication technology, bears these three layers in mind.

2.6.3 PETs and storage technology

In the context of storage technology, the focus of privacy enhancing technologies lies on ensuring an authorized access to and exchange of stored data as well as purpose bound use of stored data.

2.6.4 PETs and analysis and decision making technology

With regards to analysis and decision making, privacy enhancing data mining (PPDM) has been discussed as a privacy enhancing technology. Meints/Möller 2007 describe that currently research in this field is ‘mainly directed towards development of technical methods, such as

[90] The Open Systems Interconnection (OSI) model is a reference model developed by the International Organization for Standardization (ISO 10026-1: 1998) to describe a conceptual framework of standards for communication in a network. It is usually applied to the internet but can, with minor adjustments, also be applied to telephone networks and protocols.

application of cryptography or the development of specialised algorithms to meet security and privacy requirements for different data mining methods, such as classification or categorisation'. Privacy preserving data mining typically uses various techniques to modify either the original data or the data generated (calculated, derived) using data mining methods. Meints/Möller 2007 describe five dimensions of PPDM:

- the distribution of the basic data,
- how basic data are modified,
- which mining method is being used,
- if basic data or rules are to be hidden, and
- which additional methods for privacy preservation are used.

They conclude that focusing on algorithms and PPDM is not sufficient to implement effective privacy protection when applying data mining. Instead, a process related view has to be applied and a data protection management process has to be implemented in addition to considerations of PPDM.[91]

[91] For further discussion of product and process related models for privacy protection management see D 6.2 Criteria for privacy enhancing security technologies.

Chapter 3 PETs related design proposals

The following chapter presents technical, legal and organisational proposals regarding security technology research and design, as well as the legal bases determining the scope of use.

3.1 Technical Proposals

Technical proposals in the context of security technologies and research thereon have to address research and development institutions. The modalities of later use of the technology play an important role for the actual privacy impact. Technical proposals do therefore have to cover product and process related approaches. Considerations in a technical dimension have to be put not only on well-known aims of IT-security. These include confidentiality, integrity and availability (CIA) of data.[92] These principles are mainly applicable with regards to data transmission and storage by means of data processing systems. Many security technologies however aim at collecting data by means of sensors. The security technologies addressed by the PRISE project cover a wider range of products and not only data processing systems. A detailed derivation of product and process related proposals which are going to include technical criteria, will be a main focus of work on 'criteria for privacy enhancing security technologies'. In addition, privacy enhancing technologies, as described above, have to be taken into account when designing privacy into security technologies.

This section will thus present two examples of existing technology and process related regulations which address technical and organisational measures of data security. Privacy principles like transparency, legitimacy, or purpose binding are indirectly touched by these provisions, too. However, more specific measures for ensuring all privacy principles can be identified. This analysis will be conducted in the above mentioned report on criteria[93].

With regards to a data protection management for law enforcement authorities as later users of security technologies, the Proposal for a Council Framework Decision on the protection of personal data processed in the EC's third pillar[94] presents the following technical and organisational measures which can be applied in general to electronic data processing.

Measures shall be implemented which are designed to

- deny unauthorised persons access to data processing equipment used for processing data (equipment access control),

- prevent the unauthorised reading, copying, modification or removal of data media (data media control),

---

[92] For a detailed description see PRISE Deliverable 6.2 Criteria for privacy enhancing security technologies.

[93] PRISE Deliverable 6.2 Criteria for privacy enhancing security technologies

[94] This Commission draft framework decision has been revised by the Council of the European Union as 11365/4/07 (Rev 4), available at http://www.statewatch.org/news/2007/oct/eu-dp-draft-text-11365-rev-4.pdf

- prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control),
- prevent the use of automated data processing systems by unauthorised persons using data communication equipment (user control),
- ensure that persons authorized to use an automated data-processing system only have access to the data covered by their access authorization (data access control),
- ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control),
- ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems and when and by whom the data were input (input control),
- prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control),
- ensure that installed systems may, in case of interruption, be immediately restored (recovery),
- ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored data cannot be corrupted by means of a malfunction of the system (integrity).

These measures should be considered and technically implemented by research and development consortia who want to develop a technology which involves data storage and especially databases, as the technology has to allow compliant use.

General technical and organisational means to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and other forms of unlawful processing are also described in an annex to the German Federal Data Protection Act[95] and shall serve as an example of applying the term ‘organisational and technical measures’ as used in Article 17 section 1 of directive 95/43/EC and in Article 22 of draft framework decision 11365/4/07[96]. Regarding storage, processing and transmission of personal data, measures shall be taken

- to prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used (access control),

[95] Available in English at http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf

[96] Draft Framework Decision on data protection in police and judicial matters.

- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage (access control),
- to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (transmission control),
- to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal (job control),
- to ensure that personal data are protected from accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

Measures to ensure data security in data processing systems can be found in the Common Criteria[97], an ISO standard for information technology security evaluation. For more information refer to the Report on Criteria for privacy enhancing security technologies.

In addition to these organisational and technical measures further technical proposals to consider for enhancing privacy with regards to security technologies can be made. Some of these are addressed in draft framework decision 11365/4/07.

In order to allow later judicial scrutiny, not only the transmission of personal data should be logged or documented for the purpose of verification of the lawfulness of the data processing – as it is suggested in Article 11 of draft framework decision 11365/4/07. In addition, all access to and use of personal data, hence all processing steps of personal data should be logged. Otherwise, no efficient verification of lawfulness is possible. Significant potential of unauthorised and possibly unlawful access to and thus use of data can result from inadequate access control and not only from inadequate transmission control. If the data subject shall be granted effective legal protection a thorough picture of data processing conducted by the user is necessary.

Logging of processing and transmission does also facilitate notification of the data subject as required in Article 16 of draft framework decision 11365/4/07 and can be regarded as a transparency tool. Furthermore, a time stamp[98] on the collected data does enable an analysis at what time the technology was used and whether for example all legal requirements for using the technology were met at this point in time.

---

[97] Common Criteria v3.1 are available here: http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2

[98] Common Criteria v3.1 Part 2: Security functional components, page 147.

Data minimization is a fundamental technical requirement for security technologies. Developers of security technologies should put emphasis on how to achieve the intended aim of technology use with as little data collection and processing as possible. A security technology which does not require an excessive or extensive amount of data and still is effective in fulfilling its legitimate purpose will increase the possibility of proportionate use. In this context an additional measure would be to consider implementing automated deletion processes for data not or no longer required by law enforcement authorities. Additionally, implementing a routine for automated resubmission for checks of whether the legally permitted storage period was exceeded should be considered. Supportive measures to comply with the allowed storage period for personal data are part of a comprehensive data protection management process. A further step to technically enforce legitimacy of data processing and transmission is the development of enforceable policies which map national statutes regulating the specific data collection, transmission and use, and cannot be circumvented. Enforceable policies would make misuse of technologies as well as a function creep in use of data collected by means of security technologies more difficult. Enforceable policies require corresponding backing both from the technology as well as the receiving and transmitting authority and are therefore suitable for public authorities were system design can be ordered by means of instruction.

3.2 Legal Proposals

Currently, privacy legislation on a European level exists only within the first pillar. The draft framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (third pillar) does not touch collection of data by means of security technologies. Specific provisions regarding investigative powers and according technology use are regulated in national law and differ in scope and detail in Member States. The focus of the draft framework decision lays on privacy protection regarding exchange[99] of personal data among Member States and thus on data security issues concerning databases, stored data, access to data, and data transmission.

The following legal proposals support privacy enhancement in the context of security technology use or legislation thereof.

Member States should consider implementing a regulation of a minimum level of privacy which even for the assurance of public or state security must not be infringed or restricted (‘core sphere’).[100] Currently, considerations on limits to privacy infringement in the area of criminal investigations and preventive police measures are not dominating the discussion on anti-terror measures and measures combating organized and serious crime. Provisions defining a core sphere of privacy which is not subject to weighing of interests and proportionality considerations but which must never be infringed will strengthen the fundamental right of privacy and at the same time not affect legitimate interests of law enforcement or crime prevention. Collection of data resulting from investigations and measures touching the most

[99] See recital (6): ‘The scope of the Framework Decision is limited to the processing of personal data transmitted or made available between Member States. No conclusions can be inferred from this limitation regarding the competence of the European Union to adopt acts relating to the collection and processing of personal data at national level or the expediency for the Union to do so in the future’.

[100] See also PRISE Deliverable 3.2Legal Evaluation Report for more details.

intimate life style in a data subject's domicile should not be permissible. This claim results from the fundamental right to human dignity.

New technological advancement and development can bear new and significant risks to the right to privacy. Increasing efforts of linking personal data in order to detect plans of serious crime at an early stage of planning and subsequently prevent such plans are fostering access to data from private entities and fusing of data from various sources (for example different sensors). Constant monitoring of technical advancements and distribution of new technologies is necessary in order to assess possible need for new regulations for privacy protection. In this context specific regulations for (emerging) technologies with intense impact on privacy should be considered. In addition, a mandatory prior checking[101] of new security technologies should be introduced for public authorities during which a privacy impact assessment is carried out and alternative and possible less intrusive means of achieving the intended aim are considered.

A significant problem results from the fact that developers of technologies used for processing of personal data are not addressed by the data protection directive. Data protection law constitutes obligations for the controller, but not for the entity developing systems which the controller late uses for the collection, processing and use of personal data. Only an indirect effect on developers of security technologies results from the fact that users of security technologies (and thus the customers of security technology developers) must comply with data protection law. Controllers, even though being responsible for legal compliance, will eventually buy what is available on the market. Even though law enforcement authorities can act as drivers for technology development, no insight is available as to whether law enforcement authorities or respectively governments – when issuing a tender for development of or ordering an existing technology for a specific purpose – do not only describe the required surveillance and investigation facilitation but also requirements regarding privacy compliance and requirements. The intensity of privacy benefit is determined by the design of the security technology, the general provision allowing its use and the specific use in an investigation. It is essential that privacy requirements are taken into account already at the stage of system design.

An associated claim supporting systematic privacy impact assessment by law enforcement authorities is the introduction of a mandatory data protection management process.[102]

Prior to drafting new police laws introducing new investigative powers an assessment of necessity and effectiveness of the planned legal changes should be mandatory. Assessing the effectiveness of future powers and new security technologies to support and maintain security is very difficult from an ex ante perspective. Possible approaches towards a security impact assessment will be discussed in the Criteria Report[103]. However, expectations of security gain as a consequence of new security technology implementation and introduction of new police powers have to remain on the level of a qualitative forecast and can not be of quantitative nature. Hence a careful evaluation[104] of new police powers should be mandatory as well as the

---

[101] See Article 20 of Directive 1995/46/EC.

[102] See below and detailed description in PRISE Deliverable 6.2 Criteria for privacy enhancing security technologies

[103] PRISE Deliverable 6.2 Criteria for privacy enhancing security technologies

[104] See Ruth Weinzierl: 'Die Evaluierung von Sicherheitsgesetzen' and Marion Albers: ‚Die verfassungsrechtliche Bedeutung der Evaluierung neuer Gesetze zum Schutz der inneren Sicherheit'.

introduction of sunset clauses regulating an expiry date for law which fails to undergo evaluation or receives a negative evaluation. If an intrusive new regulation or technology turns out to be not effective, it should not prevail.

A further proposal is derived from the general legal principles of concreteness: preventive investigations without a concrete suspicion of a criminal act should be a last option and require a concrete enumeration of serious crimes which may initiate the investigative measure at question. In this context a concrete threat to significant rights should be required for computerized screening of databases and very privacy invasive measures. In order to allow judicial oversight obtaining a court order should be mandatory for covert as well as very privacy invasive measures. In addition, an obligation of notification even for covert data collection after the end of operation is necessary to ensure the data subject can seek judicial control.

3.3 Organisational Proposals

In addition to legal and technical measures and considerations regarding security technology design and use a third focus has to be put on organisational means within the using entity as well as the developing research consortium. The below presented organisational proposals focus on the research and development process as well as the FP7 funding application process. Both dimensions will be further discussed in the Criteria Report.

3.3.1 Data Protection Management Process for R&D

It is important for researchers receiving FP 7 funding to implement a method which will allow privacy compliance of ongoing research. With regards to IT products a general research and development process looks like this:

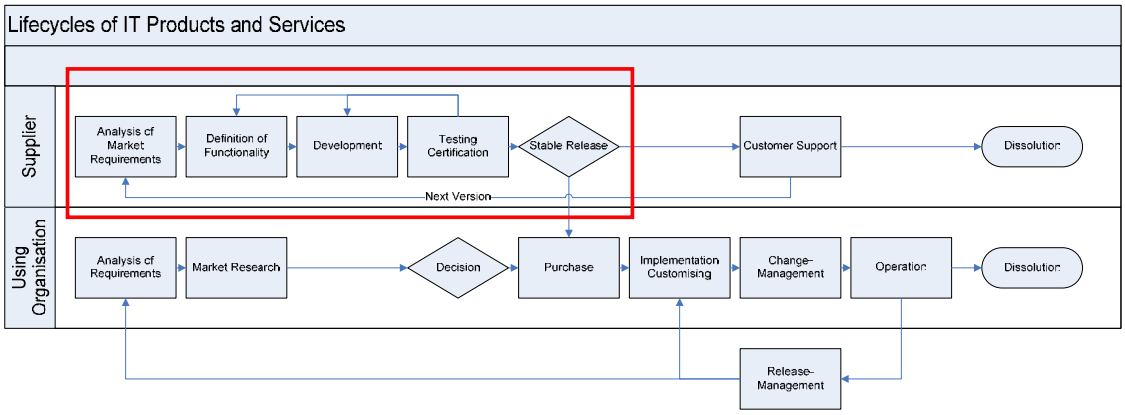

Figure 6: Research and Development process

Already at an early stage, when defining the functionality of the product/technology, considerations of privacy compliance as well as ethical compliance must be taken into account. These legal requirements include as a minimum consideration of these following data protection principles and how to comply with them:

Legitimacy: Personal data must be processed lawfully and processing requires a legal basis or the consent of the data subject.

Purpose binding: Data should be accurate and relevant to the purpose for which they are to be used. The purpose shall be specified before the data are collected and data shall not be further processed in a way incompatible with those purposes.

Proportionality: Data processed must be necessary and adequate to achieve the specified purpose.

Transparency: The data subject has to be aware of data processing taking place and of what data is being processed by which party.

Quality of the data: The personal data collected shall be accurate and, where necessary, kept up to date. Inaccurate or incomplete data shall be rectified, data no longer necessary for the specified purpose shall be erased.

Security of the data: Personal data shall be protected by reasonable safeguards against accidental or unlawful destruction or accidental loss, alteration and unauthorised disclosure.

A data protection management process applied to the research and development process would look like this:

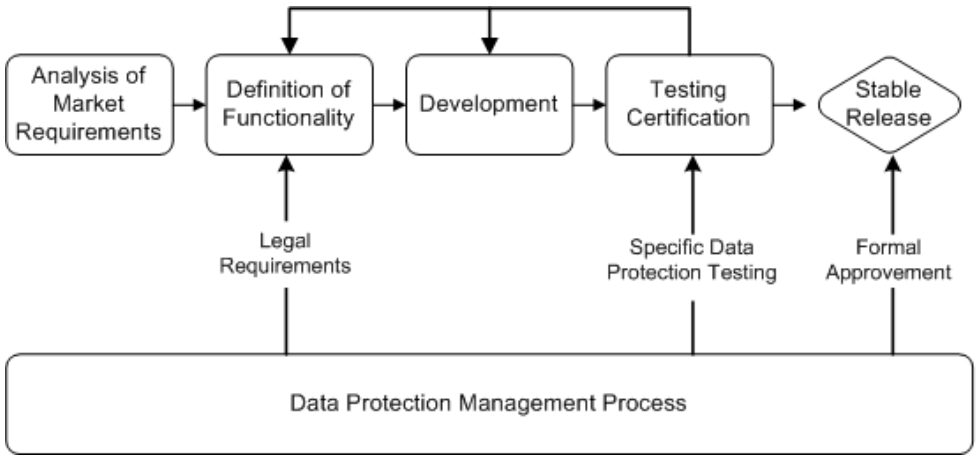

Figure 7: Data Protection Management process

In order to determine the necessary data protection and security functions, first generic and specific security targets should be listed. In a following step corresponding data protection and security functions can be identified:

- Generic and specific data security targets:
    - Complying with data protection requirements
    - Exceeding data protection requirements (best practice, PET)

- Corresponding data protection and security functions:
    - Secure logging for application and data access
    - Reminders for deleting data

When defining the functionality the following considerations have to be taken into account:

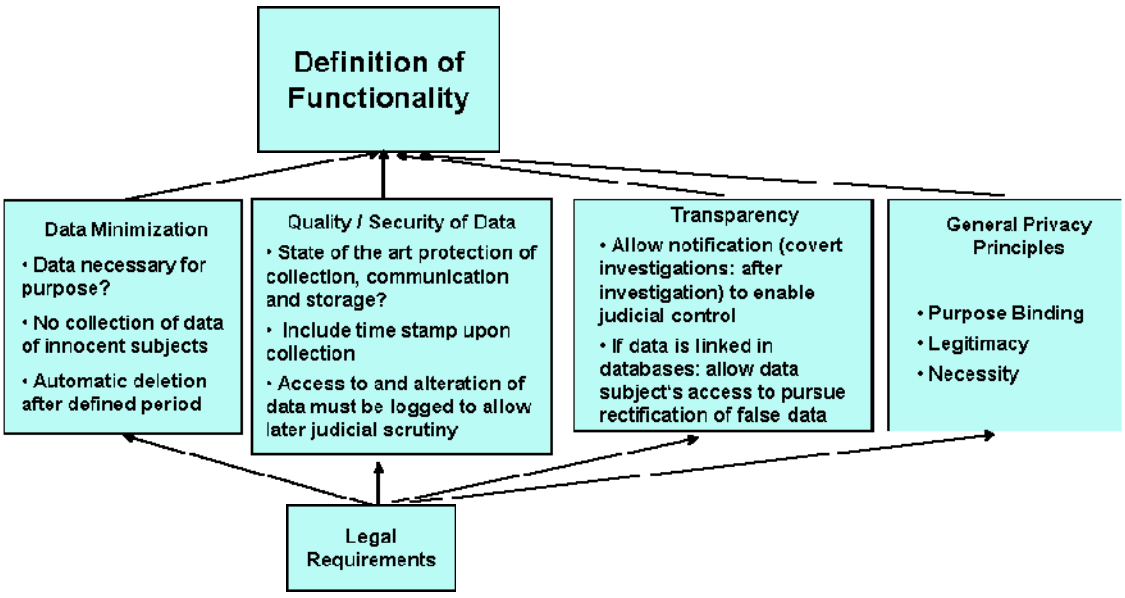

Figure 8: Privacy-friendly definition of functionality

The Criteria Report is going to present in greater detail an approach towards a data protection management process for security technologies as well as current approaches towards designing privacy into technology.

3.3.2 Organisational proposal regarding funding application

Projects aiming at research on a technology which processes personal data or data which by linking with other data can become personal data should fulfil in differenet phases the following requirements to receive funding:

During funding application phase:

PRISE will in the work on criteria for privacy enhancing technologies produce a matrix which can be used by the Commission to assess the degree of privacy risk/ level of privacy invasive orientation of the project. There may be projects that should never receive funding because they are too privacy invasive and technology use would obviously violate the proportionality principle. The developed questionnaire will also assist an assessment of security gain and privacy loss of a security technology described in a proposal applying for funding. This first evaluation of the project should have further impact on requirements the project will have to fulfil. It should be considered whether applications of projects aiming at developing their

technology in a privacy-enhancing way can expect to be favoured over those who aim only at privacy compliance. In any way, projects that are privacy relevant and don't point out in their application how compliance will be achieved – and that privacy law has been considered at all when planning the project – shall not receive funding. This is to be requested analogue to the **prior checking** regulated in Art 20 of Directive 1995/46/EC.

During the duration of the project:

All privacy relevant projects should be obliged to write a **Privacy Report** as mandatory a deliverable of the project. This is to ensure that the technical development is not conducted without taking the privacy relevant aspects of the technology in mind and to ensure privacy compliance or – even more – privacy enhancement of the technology. This report should be a public deliverable in order to achieve acceptance of the technology in public. Every citizen worried about an infringement of his privacy rights will find a detailed description on the specific technology enabling the citizen to better understand and estimate the privacy impact of the technology's functionality and what precautions and measures the developers installed to reach privacy compliance.

Additionally, those projects which don't have ethical, data protection or civil rights protection researchers in the project consortium or which process sensitive data shall be obliged to receive **privacy consulting** by an independent privacy protection authority (not by consulting companies – this is to ensure acceptance among citizens and a non-biased consulting).

At the end of the project before launch / real application of the technology

Such technologies which

- allow the collection of personal data not based on a reasonable doubt but undifferentiated of every citizen in a certain range or using a certain technology
- or the access to / mining or use of such data collected without a reasonable doubt

shall have to get an **audit/privacy seal** issued by an independent data protection authority stating that these project results (the developed technology) are privacy compliant.

Additionally an **evidence value report** shall be compulsory at the end of the project. In this report the consortium shall address the foreseeable interdependencies of the new technology with other technologies/data sources/databases and conduct a risk analysis dealing with the question what possible attacks might put the quality of the collected data at risk. What measures are taken to ensure that the data cannot be accessed, altered and manipulated?

An overview of this process would look like this:

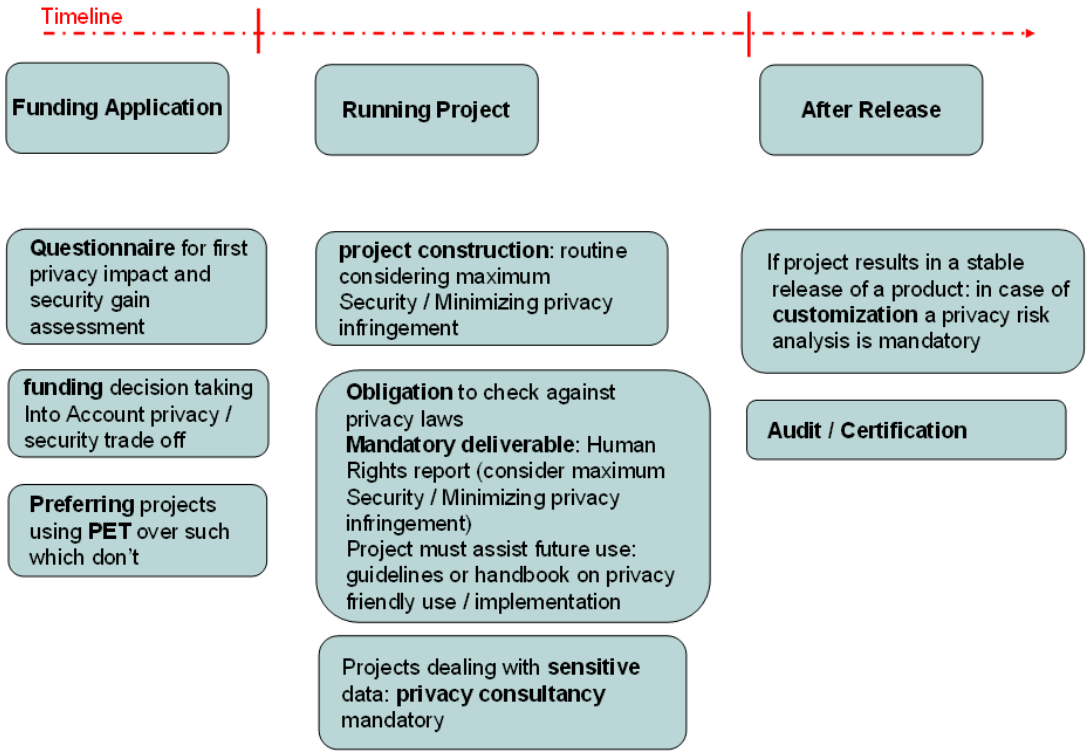

Figure 9: Timeline for a privacy-friendly research process and funding thereof

A model for assessing the privacy and security impacts of proposed security research will be presented in the Criteria Report[105].

[105] PRISE Deliverable 6.2 Criteria for privacy enhancing security technologies

Chapter 4 Conclusion

The call for PETs is a reasonable claim also for security technologies. Bearing in mind that privacy enhancing technologies fulfil the purpose of making 'breaches of the data protection rules and violations of individual's rights […] technically more difficult', the necessity to consider PETs also in the security technology context is obvious as security technologies due to their intended use comprise the probability of affecting privacy. An increased need for technical means ensuring privacy compliance exists for technologies used by law enforcement authorities.

From a legal point of view, technology development is not within scope of the data protection directive which is addressed at data controllers. This generally applies to all technologies used for processing personal data as well as for security technologies.

The Commission postulates in COM(2007) 228: 'Whilst strictly speaking data controllers bear the legal responsibility for complying with data protection rules, others also bear some responsibility for data protection from a societal and ethical point of view. These involve those who design technical specifications and those who actually build or implement applications or operating systems.'

PRISE's proposals systematically touch the product or system level as well as the organisational level. Implementing and developing privacy enhancing applications is not sufficient to enhance privacy on a large scale. In the context of security technologies also the collection of data, usually by means of sensors, should be designed in a privacy enhancing way. It is essentially the collection of data which determines data minimization. However, while entirely mechanical solutions exist which enforce data minimization[106], security technologies using sensors to collect data are often implemented in conjunction with a processor or a backend system. Data minimization is then accomplished by means of algorithms which delete or only process data relevant for the specific purpose of the technology use. On a Data Protection Management Process and product related criteria for privacy compliant security technologies, see the PRISE Criteria Report.

The general principles of privacy enhancing technologies

- Data minimization, including unlinkability, anonymity and pseudonymity
- Safeguards for personal data
- Control by the user
- Transparency of the system
- Audit and checks

[106] A simple but effective solution for CCTV is for example to limit the zoom level and the rotation angle of the camera.

are still valid also in the context of security technologies. Yet, depending on the specific investigation and procedural provisions, restrictions are possible.

During an ongoing investigation there is usually no room for control by the user, except for when he's exercising entitled rights. This may also apply to the situation after an investigation when revealing the fact that an investigation was conducted may put other investigations or officers engaged in the investigation at risk. These situations can however be expected to be an exemption and so after the end of an investigation control of the user must be enabled by means of notification.

The same goes for transparency. During an investigation, be it covert or not, transparency can not be expected to a full extend by the data subject or individuals with defined procedural roles. But if transparency cannot be ensured during the investigation, legal safeguards ensuring transparency after the end of the investigation are usually in place or should be in place. In order to allow for transparency of technology use (who used the technology when, for what purpose and was that person authorized to do so) logging of use has to be implemented. This also ensures later control by the user. Furthermore, while transparency towards the data subject is not always possible during an ongoing investigation, transparency for the security technology user and within the entity using the technology must be ensured at all times in order to facilitate legitimate use and to allow later scrutiny.

Security safeguards must always be in place protecting the collected and processed personal data. This is to be ensured not only for the benefit of the data subject. If law enforcement authorities intend to use personal data during a trial or for further investigation they have to rely on the quality of the data and the fact that the data has not been altered.

If measures supporting data minimisation are not given enough consideration, implementing security safeguards can turn out to be difficult due to the amount of data. Yet, a current tendency seems to be not on the minimization of data but rather on the expansion of data collection, processing and exchange in the context of inner security measures. This is an unfortunate political decision, which developers of security technologies may feel invited to follow.

Annex - Ethical Issues Table

The following table presents the ethical issues table currently used for FP7 proposals.[107]

	YES	PAGE
Informed Consent		
• Does the proposal involve children?		
• Does the proposal involve patients or persons not able to give consent?		
• Does the proposal involve adult healthy volunteers?		
• Does the proposal involve Human Genetic Material?		
• Does the proposal involve Human biological samples?		
• Does the proposal involve Human data collection?		
Research on Human embryo/foetus		
• Does the proposal involve Human Embryos?		
• Does the proposal involve Human Foetal Tissue / Cells?		
• Does the proposal involve Human Embryonic Stem Cells?		
Privacy		
• Does the proposal involve processing of genetic information or personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)		
• Does the proposal involve tracking the location or observation of people?		
Research on Animals		
• Does the proposal involve research on animals?		
• Are those animals transgenic small laboratory animals?		

[107] See http://cordis.europa.eu/fp7/ethics_en.html.

• Are those animals transgenic farm animals?		
• Are those animals cloned farm animals?		
• Are those animals non-human primates?		
Research Involving Developing Countries		
• Use of local resources (genetic, animal, plant etc)		
• Benefit to local community (capacity building i.e. access to healthcare, education etc)		
Dual Use		
• Research having direct military application		
• Research having the potential for terrorist abuse		
ICT Implants		
• Does the proposal involve clinical trials of ICT implants?		
I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL		

References

- Online publication
  - Albers, M: ‚Die verfassungsrechtliche Bedeutung der Evaluierung neuer Gesetze zum Schutz der inneren Sicherheit', 2006. Available at http://files.institut-fuer-menschenrechte.de/488/d48_v1_file_4486915795f82_DIM_MIR_www.pdf
  - Article 29 Data Protection Working Party: 'Opinion 4/2007 on the concept of personal data', 2007. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
  - Borchers, D: 'Terror-Schulungsraum Internet, Bürgeranwälte und die Sache mit der IP-Telefonie', 2007. Available at: http://www.heise.de/newsticker/meldung/96199
  - Cassa Mont, M. and Pearson, S. and Bramhall, P.: 'Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforcable Tracing Services', 2003. Available at http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf
  - Commission of the European Communities: 'Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) (COM (2007) 228 final', 2007. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:HTML
  - Dutch Data Protection Authority: 'Privacy Enhancing Technologies: White-Paper for decision-makers', 2004. Available at http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf
  - Grimm, R and Meissner, S et al.: 'SOAinVO – Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen', 2007. Available at http://soa-tag.uni-koblenz.de/SOAinVO-Analyse.pdf
  - Hansen, M and Meissner, S et al.: 'Verkettung digitaler Identitäten', 2007, includes executive summary in English. Available at https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf
  - Hansen, M and Pfitzmann, A: 'Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Working Document, Version 0.29', July 31 2007. Available at http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.29.pdf

- Hansen, M: 'PRIME – Privacy and Identity Management for Europe: Me, Myself and I! Managing your identities safely', 2008. Available at https://www.prime-project.eu/press_room/leaflets/Prime-Primer-2pager.pdf

- Hes, R and Borking, J [eds.]: 'Privacy-enhancing technologies: The path to anonymity, revised edition', 2000. Available at: http://www.dutchdpa.nl/downloads_av/AV11.PDF

- Hildebrandt, M: 'Profiling into the future: An assessment of profiling technologies in the context of Ambient Intelligence', 2007. Available at: http://journal.fidis.net/fileadmin/journal/issues/1-2007/Profiling_into_the_future.pdf

- Karjoth, G: 'Privacy Enhancing Technologies for RFID', slides from RFID Workshop, 2006. Available at http://www.rfidconsultation.eu/docs/ficheiros/Karjoth.pdf

- Leenes, R and Hansen, M and Schallaböck: 'PRIME white paper v2', 2007. Available at https://www.prime-project.eu/prime_products/whitepaper/

- Meints, M and Möller, J: 'Privacy preserving Data Mining', 2007. Available at: http://journal.fidis.net/fileadmin/journal/issues/1-2007/Privacy_Preserving_Data_Mining.pdf

- Moskowitz, P and Lauris, A et al.: 'White Paper – Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag', 2006. Available at http://www-03.ibm.com/solutions/businesssolutions/sensors/doc/content/bin/Clipped_Tag_White_Paper.pdf?g_type=hpfeat

- Rieback, M and Crispo, B et al.: 'Uniting Legislation with RFID Privacy-Enhancing Technologies', 2005. Available at http://www.cs.vu.nl/~ast/publications/spi-2005.pdf

- Sieker, B and Ladkin, P et al.: 'Privacy Checklist for Privacy Enhancing Technology Concepts for RFID Technology Revisited', 2005. Available at http://www.rvs.uni-bielefeld.de/publications/Reports/pet_rfid_privacy_checklist_v1.1.pdf

- Weinzierl, R: 'Die Evaluierung von Sicherheitsgesetzen – Anregungen aus menschrechtlicher Perspektive', 2006. Available at http://files.institut-fuer-menschenrechte.de/437/Policy_Paper_Die_Evaluierung_von_Sicherheitsgesetzen.pdf

- Print publications

- Borking J and Raab C: 'Laws, PETs and Other Technologies for Privacy Protection', 2001, the Journal of Information, Law and Technology.

- Camenisch, J and Lysyanskaya, A: Signature Schemes and Anonymous Credentials from Bilinear Maps; Crypto 2004, LNCS 3152, Springer, Berlin 2004, 56-72.

- Chaum, D: 'Untraceable Electronic Mail, Return Adresses, and Digital Pseudonyms', 1981, Communications of the ACM 28/10, 1030-1044.

- Chaum, D: 'The Dining Cryptographers Problem:_Unconditional Sender and Recipient Untraceability', 1988, Journal of Cryptology 1(1), 65-75.

- Chaum, D: 'Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms', 1990, Auscrypt '90, LNCS453, Springer, Berling, 246-264.

- Clauß, S and Schiffner, S: Structuring Anonymity Metrics; in: A Goto (Ed.), DIM '06, Proceedings of the 2006 ACM Workshop on Digital Identity Management, Fairfax, USA, Nov. 2006, 55-62.

- Hansen, M: ' Privacy Enhancing Technologies' in: Roßnagel, A [ed.]: 'Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung', 2003

- Hansen, M and Meints, M: 'Digitale Identitäten – Überblick und aktuelle Trends', 2006. in: DuD 9/2006, 543-547.

- Hansen, M et al.: 'Privacy-enhancing identity management', 2004, Information Security Technical Report 9(1), 35-44.

- Karjoth, G and Hunter, M: 'A Privacy Model for Enterprises', 15th IEEE Computer Foundations Workshop, 2002.

- Köhntopp, M: 'Datenschutz technisch sichern', presentation at EMR Workshop ,Allianz von Medienrecht durch Gestaltung der Informationstechnik: Ordnung in digitalen Medien durch Gestaltung der Technik – Am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltsschutz', 10.5.2001.

- Kühn, U and Lucks, S: 'Auf dem Weg zu neuen Hashfunktionen', 2007, in: DuD 8/2007, 596-600.

- Monar, J: 'Justice and Home Affairs in the EU Constitutional Treaty: What added value for the 'Area of Freedom, Security and Justice' ?, 2005, in: European Constitutional Law Journal 1(2): 226-246.

- Pfitzmann, A, Pfitzmann B and Waidner, M: 'ISDN-MIXes – Untraceable Communication with very small bandwidth overhead', 1991, 7th IFIP International Conference on Information Security, Amsterdam: Elsevier, 245-258.

- Schneier, B: 'Beyond Fear. Thinking sensibly about Security in an uncertain World', 2003, Berlin: Springer.

- Spiekermann, S and Cranor, L: 'Engineering Privacy' 2007, forthcoming.

- Working Group on "Data Protection in Telecommunications" of the Committee on "Technical and organisational aspects of data protection" of the German Federal and State Data Protection Commissioners: ‘Privacy Enhancing Technologies in Telecommunications’, 1997.

Table of figures

Table of abbreviations

Art.	article
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Office for Information Security)
BVerfGE	Bundesverfassungsgerichtsentscheidung
CCTV	Closed Circuit Television
COM	Commission
D	Deliverable
DC-Net	Dining cryptographers net
DRM	digital rights management
EC	European Communities
e.g.	exempli gratia (for example)
EPAL	Enterprise Privacy Authorization Language
et al.	et alii (and others)
EU	European Union
fn.	footnote
FP 7	Seventh Framework Programme
ID	Identity
i.e.	id est (that is)
IOI	items of interest
ISMS	Information Security System
ISO	International Organization for Standardization
IT	information technology
lit.	littera (letter)
p.	page

P3P	The Platform for Privacy Preferences
PET	Privacy Enhancing Technology
PII	personal identifiable information
PPDM	privacy friendly data mining
PRIME	Privacy and Identity Management for Europe
PRISE	Privacy and Security
RFID	Radio Frequency Identification