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

D6.2 – Criteria for privacy enhancing security technologies

2008

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

Authors:
Maren Raguse, Martin Meints, and Owe Langfeldt, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Walter Peissl, Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften

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

Contents page

Figures

Tables

Summary

This document presents criteria for data protection compliant and privacy enhancing security technologies. The aim is to identify best practice models for privacy friendly design and implementation of security technologies.

As a background for the discussion on privacy and security technologies this paper provides some input on the theoretical discussion on why privacy is a necessity to liberal democracies as well as an overview of the ongoing security discourse by analysing different security policies. Another part addresses the question whether more surveillance provides more security and whether this is necessarily always accompanied by a loss of privacy. PRISE argues that in some cases more security is possible with the same or even a higher level of privacy.

In addition to desktop research PRISE conducted interview meetings in the partner countries Austria, Denmark, Germany, Norway and in addition in Hungary and Spain. An interview meeting is a pTA (participatory Technology Assessment) procedure for gaining quantitative data from a questionnaire and qualitative data from group discussions. The PRISE approach incorporates these findings in the theoretical analysis on privacy and security and the existing know-how on deploying IT security measures and data protection management systems. Most of the conclusions from the interview meetings are therefore reflected in the three-step PRISE model.

By combining the above-mentioned inputs, PRISE has created a model and derived sets of criteria for research and development (R&D). This model – the “PRISE Matrix” – and its theoretical background will be presented in Chapter 3. It is a step-by-step approach that leads to privacy-compliant or privacy-enhancing systems-design of new security technologies.

A core part of this report is the presentation of techno-organisational measures to achieve data protection compliance and privacy-enhancing solutions. Finally in Chapter 4 we present two A4-forms: one for proposal writers and one for evaluators to assess data protection compliance and the social impact of new security technologies. In the PRISE handbook we finally provide guidance on how to solve problems concerning privacy issues that might arise during the technology development process.

1 Introduction

This document presents criteria for data protection compliant and privacy enhancing security technologies. The aim is to provide guidance for best practice models on the privacy friendly design and implementation of security technologies based on the following prior work:

- the results of an analysis of privacy enhancing design principles[1], and
- the general public attitude towards security derived from the interview meetings conducted by the PRISE project in 6 European countries[2].

Of importance in the background to the discussion on security technologies are the different security policies. PRISE provides an overview of this discourse by analysing these policies. Another important discussion is whether more surveillance really provides more security and whether this is necessarily accompanied by a loss of privacy. PRISE argues for proportionality and that more security is possible with the same – or even a higher – level of privacy in some cases.

By combining the above-mentioned input, PRISE has created a model and derived sets of criteria for research and development (R&D). This report is based on discussions in a group with different stakeholders from research, industry and government agencies[3].

Basically, PRISE aims at developing criteria which are applicable in different areas of application as well different stages of development (research, development, implementation) and by different actors (research coordinators, industry, policy makers, public and private users). The main focus is the applicability of the PRISE model within the writing and evaluation of FP7 proposals.

It is often said that privacy and security are antagonisms and may only exist in the form of a trade-off or a zero-sum game. In order to clarify the relationship between the two, we first discuss the concept of and the right to privacy from different perspectives and provide some insight into different security discourses. After the theoretical discussion of concepts of privacy and the security discourse in the EU, we present a methodology for deducing the criteria for privacy enhancing security technologies. This results in two very short checklist-like forms, one for proposal writers in R&D, and one for the evaluators of such proposals. These two A4-forms are supplemented by a handbook which sets out hints and recommendations on tools for fulfilling the requirements of the above-mentioned criteria.

The right to privacy is prominently regulated in national and international law.[4] In many European countries it is a fundamental right protected by the constitution. Chapter 2.1 provides a very short overview. Privacy can also be seen as a fundamental pillar of liberal democracy

---

[1] Details see D3.3 Proposal Report

[2] Austria, Denmark, Germany, Hungary, Norway and Spain. For details see D5.8 Synthesis Report

[3] Discussions took place throughout the project but focussed on two user and stakeholder workshops. The first held in Copenhagen 29th January 2007 and the second in Vienna 4th February 2008.

[4] A detailed description of the international regulation can be found in D3.2 Legal Report

and as a social value in itself. Arguments for privacy from a democratic perspective are given in Chapter 2.2. The following Chapter 2.3 discusses the question of whether there is a trade-off between privacy and security. In recent years we have seen a discussion of new security concepts, shifting the focus from a classical state-orientated "National Security" approach to a "Human Security" approach that is more focussed on individual rights (first published by the UNDP). Chapter 2.4 gives an overview of the different concepts of security.

Taking this into account in the R&D of security technologies means that security technologies should be designed in a way that as far as possible ensures that changes in social and/or political systems do not make them intrusive. Even without dramatic changes in society we must be aware that implementing and using security technologies in certain ways may influence society. Widespread surveillance may shape attitudes and behaviour. Lowering legal barriers to data surveillance may shift the general value of the individual's privacy. The interdependence between technological and social development makes it necessary to think about the conditions of actual use and implementation of technology as well as the long-term development processes in society. What we call for is a precautionary principle in developing and implementing security technologies.

The PRISE model

The basic idea of the PRISE model is a step-by-step approach from privacy compliant to privacy enhancing technologies.

1. All new security technologies have to comply with a minimum baseline. This means there is a core sphere of privacy that should never be intruded into under any circumstances.

2. New security technologies should comply with existing privacy laws.

3. Security technologies should be designed according to principles for privacy enhancing technology (PET)[5].

PRISE also discusses what other dimensions should be taken into account when analysing a security research proposal in the FP7 programme. Even if the research planned and laid down in a security call proposal within FP7 as such complies with privacy requirements, a project could be rejected for other reasons. If a security technology cannot facilitate any gain in (societal) security, or even reduces an individual's security, it should not receive funding, even if the technology would be privacy compliant as such.

PRISE therefore suggests applying an assessment to security research proposals submitted. This PRISE approach will describe a methodology for evaluating the legal compliance and social impact of a research proposal. The approach will provide detailed assistance on different phases of research and development:

[5] For an in-depth description of privacy enhancing technologies in the context of security technologies see D3.3 Proposal Report.

- Which questions need to be addressed when assessing the impact of security research during the application process (plan)?

- What criteria should a security research consortium consider in order to develop a legally compliant and socially acceptable technology (build)?

- How can a consortium provide measures to ensure that a future user will use the technology in the least infringing way (run).

The presented approach provides a set of questions to guide the research project evaluation, complemented by detailed discussions of the underlying aspects. The approach will be presented in detail in Chapter 3. On the basis of this approach we designed the PRISE-Matrix, including a version condensed into two A4-forms (Chapter 4). These forms guide proposal writers as well as evaluators quickly through the main questions and give hints on whether a technology fits the criteria or not. For main aspects we also provide measures to resolve conflicts with the PRISE criteria. These measures are collected in the PRISE-Handbook (Chapter 4.3).

2 Privacy and security: Basic needs for individual and society

2.1 Privacy as a fundamental right

Privacy is a concept that is essential from various perspectives. It has anthropological, sociological, philosophical and political roots and notions. Although a commonly agreed definition is not available there are several attempts to describe it[6]. The idea of privacy is based on the differentiation between individuals and others and their private and the public sphere. The concept of privacy is strongly influenced by liberalism and the idea of "civil society comprised of relatively autonomous individuals who need a modicum of privacy in order to be able to fulfil the various roles of the citizen in a liberal democratic state". (Raab/Bennett 2003, 14)[7] Because of the liberal bases and the fact that what is regarded as private is strongly dependent on cultural and individual perceptions, the individual himself plays an important role in this concept. A well-known notion of privacy is "the right to be left alone", a definition by Warren/Brandeis[8] in their 1890 paper . Another important term in this respect is the notion of "informationelle Selbstbestimmung" (informational self-determination), which arose after a ruling of the German Constitutional Court in 1983.[9]

Privacy is a broad concept, which consists of the freedom to decide on private issues, the informational privacy to control who knows what about one's self, and the local privacy of the home.[10] With respect to the issue at stake we mainly deal with informational privacy. This could be roughly described as the claim to control the flow of one's own personal information. In order to make this operational, a set of rules were developed and fed into national and international regulations. Data protection is therefore an instrumental core part of the broader concept of privacy.

The right to privacy is well regulated in national and international law.[11] In many European countries it is a fundamental right protected by the respective constitutions. At the international level there are a number of regulations that acknowledge the right to privacy as being fundamental. These provisions can for example be found in the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (known as Convention 108). All EU Member States have ratified this Convention, which lays down data protection as a part of the protection of fundamental rights and in particular the individual's right to privacy. The Lisbon Treaty contains a reference to fundamental rights in Article 6 of the Treaty of the European Union[12] and seeks to incorporate them as 'general principles' into Union law.

---

[6] For good overviews see: Bennett, C. J. und Raab, C. D., 2003, The Governance of Privacy, Aldershot, Hampshire GB: Ashgate and Rössler, B., 2001, Der Wert des Privaten, Frankfurt am Main: Suhrkamp

[7] Bennett, C. J. und Raab, C. D., 2003, p 14.

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

[9] BVerfGE, Volkszählungsurteil, 65(1), 42f

[10] see Rössler, B., 2001, Der Wert des Privaten, Frankfurt am Main: Suhrkamp

[11] A detailed description of the international regulation can be found in D3.2 Legal Report

[12] The Lisbon Treaty is available at http://www.consilium.europa.eu/uedocs/cmsUpload/cg00014.en07.pdf

However, it can still be asked why privacy receives such a strong legal protection. There is good reason for this. A central argument is the philosophical argumentation for liberal democracies. One of the core elements of a democratic society is the free and autonomous citizen; and both freedom and autonomy is are closely interlinked with privacy. To be free means to decide autonomously, complying only with one's own free will, which is possible only in isolation. Living together always means considering other members of society and acting within the legal and moral framework. However this emphasises the fact that the ideal autonomous citizen forms the basis of liberal democracies. But anyone who is aware that they are under surveillance is no longer acting freely. The loss of autonomy leads to a loss of authenticity of behaviour – to "estranged behaviour" (Rössler 2001, 233)[13] In other words awareness of surveillance makes people act "as if" (ibid.). The lack of means to control the disclosure of personal data will force people to avoid attracting attention ("chilling effect"). This decrease of autonomy endangers other important pillars of democracy: freedom of speech, freedom of assembly and freedom of information. These fundamental rights form the basis for political discourse, pluralism and transparency. The right to privacy is therefore a kind of prerequisite for other fundamental rights and thus for liberal democracy.[14]

Besides the liberal "privacy paradigm" there are other approaches that argue in favour of privacy as a social value in itself. A definition of democracy such that participation, cooperation and community consciousness are considered to be its benchmarks opens up the argument that being under surveillance – which means losing information privacy and autonomous space – leads to an erosion of political participation and discourse. Similarly, excessive surveillance may lead to an erosion of trust, an exacerbation of risks and to social inequalities (see Raab and Bennett, 2003)[15].

Besides legal, philosophical and political arguments for privacy, there is also anthropological and psychological evidence of the value of privacy. Many different studies show that the distinction between private and public is a fundamental need for individuals.[16]

2.2 Privacy from a democratic perspective

In the new emerging field of surveillance studies (see Lyon 2003 and 2007, Zurawski 2007)[17] the focus of research is on the impact of surveillance. It also provides some useful insights for the discussion on privacy and security . One of the strong hypotheses is about social sorting. This means that people under surveillance are classified by their virtual patterns of behaviour and by specific criteria of classification. Or as Lyon (2003) puts it: "For surveillance today

---

[13] Rössler, B., 2001, Der Wert des Privaten, Frankfurt am Main: Suhrkamp.

[14] In addition to the argument that privacy is necessary for democracy, there is also the contention that it has an instrumental value. The proper implementation of privacy rules increases the chance that the right people use the right data for the right purposes. Privacy protection has an instrumental value and ensures that other rights are not jeopardised.

[15] Bennett, C. J. und Raab, C. D., 2003, The Governance of Privacy, Aldershot, Hampshire GB: Ashgate.

[16] See Gridl, R., 1999, Datenschutz in globalen Telekommunikationssystemen; in Reihe: Frankfurter Studien zum Datenschutz, Bd. 12, ed. Simitis, S., Baden-Baden: Nomos Verlagsgesellschaft, FN 19 p19; Egger, E., 1990, Datenschutz versus Informationsfreiheit – Verwaltungstechnische und verwaltungspolitische Implikationen neuer Informationstechnologien; in Reihe: Schriftenreihe der Österreichischen Computer Gesellschaft, Bd. 52, ed. OCG, Oldenbourg, Wien, München: Oldenbourg, FN2 p67; Elias, N., 1978, Über den Prozeß der Zivilisation. Soziogenetische und psychogenetische Untersuchngen. Bd I: Wandlungen des Verhaltens in den weltlichen Oberschichten des Abendlandes; Bd. II: Wandlungen der Gesellschaft. Entwurf einer Theorie der Zivilisation.: Suhrkamp Taschenbuch.

[17] See Lyon, D. (Ed.), 2003, Surveillance as Social Sorting. Privacy, Risk and Automated Discrimination, London: Routledge, Lyon 2007, Surveillance Studies An Overview, Polity and Zurawski, N. (Ed.), 2007, Surveillance Studies Perspektiven eines Forschungsfeldes, Opladen: Verlag Barbara Budrich.

sorts people into categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice." But surveillance still can be seen as a trigger for adapted individual behaviour. The panoptic society can be traced back to the well-known Panopticon of Jeremy Bentham, who modelled a prison in which the prisoners could be observed from a central point, but were not able to see the observers themselves. Foucault (1994, 258)[18] pointed out that the specific meaning of this model lies in the creation of a permanent awareness of being observed that ensures that power takes effect automatically. In other words, the effects of surveillance are permanent even if there is no actual surveillance. Foucault transferred the mechanisms of the Panopticon to describe modern societies. Today, it is used to describe the new kind of transparency in the information society (Rössler, 2001, 219)[19].

In the long run, a much greater problem may arise: The short-term "mainstreaming" of citizens' behaviour, i.e. restricting variation and avoiding what would be deemed deviation, may turn out to reduce the "driving momentum" in social, cultural and economic terms (Peissl, 2003)[20]. Dissenting or variant behaviour is considered to be one of the most important driving forces of economic and social development. If this force is lost, Western democratic societies may face an erosion of the core values they are built upon. In the social sciences, it is widely acknowledged that non-conformist behaviour is a necessary driving force for social development. And conflict is the great and creative power that promotes social change (Dahrendorf, 1965, 109 in Endruweit, 1989, 803)[21].

The same kind of reasoning is also used in economic theory. An example is the notion of "entrepreneur" in Schumpeter's writing. According to Schumpeter, entrepreneurs are economic agents whose function is "the carrying out of new combinations, the creative destruction of *equilibria*, thereby preparing the ground for a superior state of equilibrium." (Swoboda, 1984: 17)[22]. This is not the place to go into the details on Schumpeter's theory but the following quotation represents part of his theory cited here: "While an economic subject swims with the stream in the well known cycle, it swims against the stream if it wants to change its way." (Schumpeter, 1952: 118/transl. by the author)[23]

The purpose of this was to show that social, economic and cultural change is important for social development and, following the precautionary principle, we need to be aware of possible long-term implications of mainstreaming, which might be a side effect of restricting citizens' privacy.

---

[18] Foucault, M., 1994, *Überwachen und Strafen. Die Geburt des Gefängnisses*, Frankfurt/Main: Suhrkamp.

[19] Rössler, B., 2001, *Der Wert des Privaten*, Frankfurt am Main: Suhrkamp.

[20] Peissl, W., 2003, Surveillance and Security – a dodgy relationship., Journal of Contingencies and Crisis Management 11(1 March 2003), 19-24.

[21] Endruweit, G., 1989, Wandel, sozialer, in: Endruweit, G. und Trommsdorf, G. (Ed.): *Wörterbuch der Soziologie*, Stuttgart: Enke, 798-805.

[22] Swoboda, P., 1984, Schumpeter's Entrepreneur in Modern Economic Theory, in: Seidl, C. (Ed.): Schumpeterian Economics – Schumpeter Centenary Memorial Lectures Graz 1983, Berlin/Heidelberg/New York/Tokyo: Springer, 17-30.

[23] Schumpeter, J., 1952, *Theorie der wirtschaftlichen Entwicklung – Eine Untersuchung über Unternehmergewinn, Kapital, Kredit, Zins und den Konjunkturzyklus*, 5. Aufl., Berlin: Duncker & Humblot.

2.3 Is there a trade-off between privacy and security?

A dominating assumption in security policy discourse is that more security could be gained by more surveillance. If that is true and more surveillance necessarily leads to less freedom, it would be true that more security means less freedom (privacy). To challenge this, we need to answer two questions (a) does more surveillance always lead to more security and (b) does more surveillance necessarily lead to less privacy?

The first question will be dealt with later in this chapter. The fundamental objective of the PRISE-project is to provide guidance to answering the second question in the negative. The project aims at defining criteria for privacy enhancing security technologies – to make it possible to design and use security technologies without or at least with less impact on privacy. In our concept, privacy and security can no longer be seen as a zero-sum game.

Many security technologies are used for surveillance. They deal with norm behaviour and perceived risks from human beings with non-conforming attributes. Since the attacks of 9/11 and those in London and Madrid, security measures have been set up throughout Europe aimed at raising security for European citizens. These measures are based on the reasoning that more surveillance leads to more security.

With regard to the following discussion, security is defined as both (a) the security of individuals and (b) the security of society and the state. Security for individuals means a state in which there is no immediate or concrete risks of an infringement of the individual's protected legal rights (e.g. property, physical integrity, life, freedom). There is always a general risk of an infringement of all legal positions held by an individual , which cannot be reduced to zero if an individual participates in social interaction with other individuals, legal persons or the government. It is therefore not possible to ensure a state of 100% security with no general or concrete risk for an individual's legal rights. The security of society would mean that there is no risk of an act threatening the foundations of society. Acts threatening the foundations of society comprise for example terrorist attacks or punishable actions affecting a large or unknown number of citizens as well as attacks against a state's critical infrastructure. It would be necessary to control every individual's actions at all times in order to assure 100% security of society.[24]

It is helpful for the assessment to distinguish between an ex-ante and an ex-post perspective. If new surveillance technologies contribute to identifying potential terrorists before they can perform their criminal activities, this would increase individual and societal security. Surveillance and risk analysis can be defined as a sequence of acts of control, comparing an actual behaviour with standardised behaviour – however defined. However, it is difficult to detect planned attacks and unlawful acts beforehand and to reliably prevent such plans. This is true of telecommunications wiretapping and eavesdropping as well as of video surveillance of public places and of the biometric methods that are being discussed all over the world. Electronic fingerprints or iris scans can only say something about the authenticity of a person. However, if an individual has not attracted attention yet, he or she will probably not be in a police authority's database and therefore can hardly be identified as "suspicious". In an attempt to predict and detect suspicious behaviour and plans, the design of data fusion and analysis

[24] See Di Fabio, U. , 2008, *Sicherheit in Freiheit*, Neue Juristische Wochenzeitschrift No. 7/2008.

tools is currently being put forward.[25] Such tools would link data from many different sources and try to identify patterns of unusual behaviour. The efficiency and reliability of such tools is as yet unknown. While it seems for example possible to develop algorithms which allow for the detection of listed suspicious "keywords" and even the detection of suspicious bank transfers, the use of such a tool in order to establish a suspicion against a potential perpetrator is currently not covered by all EU member states' legal framework. A ruling of the German Constitutional Court from 2006 on the law enforcement power to conduct "dragnet investigations (Rasterfahndung)"[26] lays down strict thresholds for the use of such a tool in Germany. It should be noted that the use of data fusion and analysis tools to detect suspicious behaviour to prevent an intended unlawful action bears a high risk of false positives. It is therefore unclear whether more surveillance of the general public is an efficient means for prevention as compared with focused surveillance activities based on concrete suspicion or whether a negative effect prevails from increasing the haystack in which the needles are hidden and shifting resources from law enforcement to unusual but not harmful behaviour. Thus we can conclude from an ex-ante perspective that, in general, surveillance can but does not necessarily always raise security.

From an ex-post perspective, data sets gained from huge databases and widespread surveillance can certainly facilitate the prosecution of criminals. Deterrence, i.e. the positive impact of high rates of reconnaissance and high penalties, can be enhanced, and the persons or networks behind the attackers may be uncovered. However, deterrence cannot prevent people from performing terrorist attacks, especially if they are willing to risk their lives anyway.

Further factors limit the effectiveness of widespread surveillance. As soon as technical means like CCTV systems in public places or the retention of telecommunication systems traffic data is perceived by the general public (and criminals), they will try to circumvent those surveillance systems by (i) strategies of avoidance and/or (ii) use of preventive technologies. Strategies of avoidance may be the shift of criminal activities to unobserved areas or the use of personal communication and meetings rather than digital communication and virtual meetings like phone calls, e-mail or chat-rooms. Preventive technologies like steganography require specific know-how, and anyone has the resources, the education and the determination to do so will be able to remain incognito. Most probably, criminals will do so and it will tend to be the "ordinary citizens" who are traced and restricted in their basic freedom and fundamental right of privacy.

More surveillance does not necessarily lead to a higher level of societal security. Hence there must be a thorough examination of whether the resulting massive constraints on human rights are proportionate and justified.

The overall aim of PRISE in this context is to provide guidance for the development of technologies that provide both: more security and more privacy.

---

[25] An example is reported research of Siemens regarding an „Intelligence Platform" which would allow fusing data from all thinkable sources and conducting an analysis aiming at detecting suspicious behaviour. See ORF Futurezone, 31.3.2008. Available at http://futurezone.orf.at/it/stories/267116/.

[26] BVerfG, 1 BvR 518/02 vom 4.4.2006, Absatz-Nr. (1 - 184), http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html

2.4 Security

2.4.1 Definitions and concepts

Security is a multi-facetted phenomenon and means different things to different people. It varies considerably from one scientific discipline to another and in the broader context of public and political debate. Basically, security derives from the Latin "securus", which itself is based on "sine" (without) and "cura" (concern/worry/problem). This means security may be defined as the status of no necessity to care (see Weinandy 2007)[27]. It is the absence of danger to individuals as well as to institutions. Because there is no situation without any danger or threat from outside, security is the condition of being protected against danger or loss. (Wikipedia 2007)[28]

In the course of time security has been loaded with different dimensions.[29] Since the 18th century security has included the protection of individuals, their rights and property. In 1948 the Universal Declaration of Human Rights[30] stated in Article 3 "Everyone has the right to life, liberty and security of person." And in Article 22 "Everyone, as a member of society, has the right to social security and is entitled to realisation, through national effort and international co-operation and in accordance with the organisation and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality."

In the context of the PRISE project we defined security as the absence of danger – that is a state where the desired status quo is not threatened or disrupted in any way. Furthermore, in PRISE, security is understood as the security of society – or more precisely – of the citizens that constitute society. (PRISE 2007)[31]

Security has a twofold character: it is the security of society – organised in national states – and it is the security of the individuals forming a society. This twofold character of security will be further elaborated in the next paragraphs dealing with widely acknowledged concepts of security.

2.4.2 National Security

There is a long tradition of security policy based on Hobbes' contribution to state philosophy, which saw the protection of the individual's security as a responsibility of the state. In that sense security prevailed over freedom.[32] Traditional state-centred security was the dominating concept and reached a peak during the Cold War. "For forty years, the major world powers entrusted the security of their populace, and to a certain extent of the world, to a balance of power among states. … This type of security relied primarily on an anarchistic balance of power (power as the sole controlling mechanism), the military build-up of two superpowers, and on

---

[27] Weinandy, K., 2007 Sicherheitsforschung das Geschäft mit der Angst. Die Rolle der Ökonomie im (Un)Sicherheitsdiskurs. Eine kritische Betrachtung. Unpublished manuscript, Vienna.

[28] http://en.wikipedia.org/wiki/Security Site visited 9th December 2007

[29] For details see: ÖAW (2005): Sicherheitsforschung, Begriffsfassung und Vorgangsweise für Österreich, 20ff

[30] http://www.un.org/Overview/rights.html

[31] D2.2 Overview of security technologies v1.1, July 2007

[32] R. Ullman, 1983, Redefining Security, International Security, vol. 8, no. 1, 129-153; and Thomas Hobbes, The Leviathan cit in: Taylor OWEN (2004) Challenges and opportunities for defining and measuring human security in HUMAN RIGHTS, HUMAN SECURITY AND DISARMAMENT, disarmanet forum 2004 Vol three.

the absolute sovereignty of the nation-state. … Security was seen as protection from invading armies; protection was provided by technical and military capabilities; and wars were never to be fought on home soil – rather, proxy wars were used if direct combat were necessary." (Owen 2004, 16)[33] After World War II, diplomacy and international organisations began to play a more important role; organisations like the United Nations were widely acknowledged for dispute resolution. (ÖAW 2005, 23). The Helsinki Final Act of the Conference for Security and Cooperation in Europe (CSCE, 1975)[34] established 10 basic principles (see Tretter 1984[35] cit. ÖAW 2005, 23). "Respect for Human Rights and Fundamental Freedom" was among them. Although security policy was state-centred for a long time, at least there remained a marginal aspect of security for individuals.

2.4.3 Human Security Concept

In recent years a new approach has become more important in the political sphere and centres the focus more on the individual than on the national state. In 1994 the UNDP published the new concept of human security in its *Human Development Report.* This document is generally seen as the first significant attempt at articulating the broad approach to human security as a part of international policy. The report describes human security as having two principal aspects: the *freedom* from chronic threats such as hunger, disease and repression, coupled with the *protection* from sudden calamities (see Owen 2004, 18). The report identifies seven components of human security:

- Economic security threatened by poverty;
- Food security threatened by hunger and famine;
- Health security threatened by injury and disease;
- Environmental security threatened by pollution, environmental degradation and resource depletion;
- Personal security threatened by various forms of violence;
- Political security threatened by political repression;
- Community security threatened by social unrest and instability. (United Nations Development Programme, 1994)[3637]

With the human security concept, the individual-centred approach entered into academic and political discussions. The first "broad" approach was influenced by development policy. Further discussions gave rise to other approaches leading to a "narrow" definition of human security that primarily focused on violent threats. The narrow approach towards human security "restricts the parameters of human security to violent threats against the individual. This can come from a vast array of threats, including the drug trade, landmines, ethnic discord, state failure, trafficking in small arms, etc." (Owen 2004, 19).

---

[33] Owen, T., 2004: Defining and measuring human security, *Human Rights, Human Security and Disarmament*, three 2004, 15-24.

[34] Conference on Security and Co-operation in Europe (CSCE) 1975, Helsinki Final Act, Download: http://www.osce.org/item/4046.html

[35] Tretter, H. (ed.) (1984): KSZE. Die Abschlussdokumente der Konferenz für Sicherheit und Zusammenarbeit in Europa. 1975 und der Nachfolgekonferenzen Belgrad 1978 und Madrid 1983, Wien.

[36] United Nations Development Programme, 1994, 'New Dimensions of Human Security', *Human Development Report 1994*, New York, Oxford University Press, pp. 22–25.

[37] As summarized in Andrew Mack, forthcoming, 'Data Issues' cit. in Owen 2004.

In order to be able to measure the level of human security Owen provides new definition. In his proposal "Human security is the protection of the vital core of all human lives from critical and pervasive environmental, economic, food, health personal and political threats." (Owen 2004, 20).

The following table (Owen 2004, 17) gives an overview on different approaches to security:

Type of security	Referent object	Responsibility to protect	Possible threats
Traditional security	The state	The integrity of the state	Interstate war Nuclear proliferation Revolution
Human security	The individual	The integrity of the individual	Disease Poverty Natural disaster Violence Landmines Human rights abuses

Table 1: Traditional and human security

2.4.4 Security concepts of the EU

Security policy on the level of the European Union has only recently been established[38]. Beginning with the Maastricht Treaty on the European Union in 1992, the establishment of the second (Common Foreign and Security Policy) and third (Justice and Home Affairs) pillars created the basis for European security policy. In 1997 The Amsterdam Treaty was signed and EU military capability was introduced to European Security and Defence policy (ESDP). In 2003 the EU convened the Group of Personalities and adopted the European Security Strategy (ESS), which is set out in "A secure Europe in a better world" (2003)[39]. The strategy states that "Large-scale aggression against any Member State is now improbable. Instead, Europe faces new threats which are more diverse, less visible and less predictable." (ibid, 3) Consequently it addresses five key threats for European security: terrorism, proliferation of weapons of mass destruction, regional conflicts, state failure and organised crime. These key threats have to be addressed and it is wise "to be ready to act before a crisis occurs. Conflict prevention and threat prevention cannot start too early" (ibid 7)

The strikingly new in the strategy is the fact that "new threats" are not pure military and cannot be tackled purely by military instruments. A mixture of instruments is envisaged and this leads to the concept of dual use. This was stated clearly in the Group of Personalities Report "Research for a Secure Europe" in March 2004[40]. Other strategic objectives of the European Security Strategy aim at "building security in our neighbourhood", acknowledging the

[38] For a overview see: B. Hayes (2006): Arming Big Brother – The EU's Security Research Programme, Transnational Institute, TNI Briefing series 2006/1

[39] A Secure Europe in a Better World – European Security Strategy *(ESS – 12/2003) see:* http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/reports/78367.pdf

[40] Group of Personalities Report "Research for a Secure Europe", March 2004 see: http://europa.eu.int/comm/enterprise/security/doc/gop_en.pdf

importance of the United Nations Charta as a fundamental framework for international relations. The EU has therefore opted for “an international order based on effective multilateralism”.

The policy implications are outlined as follows: Europe’s role in a globalised world should be more active, more capable, more coherent and aimed at working with partners (ESS 2003). After the adoption of the ESS the Group of Personalities (GoP) in the field of security research published the report on “Research for a secure Europe”, which formed the basis for the Preparatory Action on Security Research and the Security research area in FP7 later on. In April 2005 the European Security Advisory Board (ESRAB)[41] was established. This Board was set up to make recommendations to the Commission in the following areas:

- the strategic missions, focus areas and priority setting for future security research programme, on the basis of the report “Research for a Secure Europe” of the Group of Personalities while taking into account the establishment of the European Defence Agency as well as national and inter-governmental activities;
- the technological capabilities to be put in place among the European stakeholders; it shall recommend a strategy to improve the European industry’s technological base so as to improve its competitive ability;
- the strategic and operational aspects of the future security research programme taking into account the experience and results obtained from the Preparatory Action on the enhancement of the European industrial potential in the field of security research, from Commission services with an active interest in the field of security including research covered by the EC Framework Programme for research and from other expert or advisory groups ;
- the implementation issues such as the exchange of classified information and intellectual property rights;
- optimising the use of publicly-owned research and evaluation infrastructures;
- a communications strategy to promote awareness of the future security research programme as well as for providing information on stakeholders’ research programmes.

In September 2006 ESRAB published the final report "Meeting the Challenge"[42], setting the European security research agenda, thereby structuring the forthcoming research on security within FP7.

Besides these formal documents from EU bodies there was an attempt to incorporate the human security concept into European policy. The so-called Barcelona Report[43] was written by members of the private Study Group on Europe’s Capabilities and presented to the EU High Representative for Common Foreign Affairs and Security Policy Javier Solana in September 2004. It was an attempt to launch a discussion on Human Security as a part of the EU’s Foreign Affairs and Security Policy. The report proposes a “Human Security Doctrine for Europe”. The authors refer to human security as the “freedom for individuals from basic insecurities caused by gross human rights violations.” (Study Group 2004)

---

[41] http://ec.europa.eu/enterprise/security/articles/article_2006-04-06_en.htm

[42] http://ec.europa.eu/enterprise/security/articles/article_06_09_25_tc_en.htm

[43] The Study Group on Europe’s Security Capabilities (2004): Human Security Doctrine for Europe http://www.lse.ac.uk/Depts/global/Publications/HumanSecurityDoctrine.pdf

The doctrine comprises three elements:

- A set of seven principles for operations in situations of severe insecurity that apply to both ends and means. These principles are: the primacy of human rights, clear political authority, multilateralism, a bottom-up approach, regional focus, the use of legal instruments, and the appropriate use of force. The report puts particular emphasis on the bottom-up approach: on communication, consultation, dialogue and partnership with the local population in order to improve early warning, intelligence gathering, mobilisation of local support, implementation and sustainability.

- A 'Human Security Response Force', composed of 15,000 men and women, of whom at least one third would be civilians (police, human rights monitors, development and humanitarian specialists, administrators, etc.). The Force would be drawn from dedicated troops and civilian capabilities already made available by member states as well as a proposed 'Human Security Volunteer Service'.

- A new legal framework to govern both the decision to intervene and the operations on the ground. This would build on the domestic law of host states, the domestic law of sending states, international criminal law, international human rights law and international humanitarian law. (Study Group 2004, 5)

The report aims at giving the Foreign and Security Policy of the EU a new direction through the incorporation of the Human Security Concept.

However, critics say that "the authors of the Barcelona Report are not primarily interested in reflections about the concept of human security. They regard this term more or less as a valuable tool, which helps them to elaborate an alternative, partly avantgardistic foreign and security policy for the European Union." (von Bredow 2005, 1)[44]

The Barcelona Report gives three reasons why the European Union's security policy should be based on human security approach:

1) Morality: Our common humanity calls for equal treatment and the right for every human being to live with dignity and security. Furthermore, this means an obligation to help each other when that security is threatened.
2) Legality: If human security is considered as a narrower category of the protection of human rights, as proposed above, then it is now generally accepted that other states, and international institutions such as the EU, have not only a right, but also a legal obligation to concern themselves with human security worldwide.
3) "Enlightened self-interest": The whole point of a human security approach is that Europeans cannot be secure while others in the world live in severe insecurity. (Study Group 2004)

The scope of PRISE deals with the development and implementation of inner security measures within Europe, from a global technology transfer perspective. The European Security Strategy as well as the Human Security Doctrine for Europe states the necessity of intervening outside the EU to protect the security of EU citizens. PRISE aims at giving advice to decision

[44] The Barcelona Report on a Human Security Doctrine for Europe, Overview and Some critical Remarks. Berlin Symposium on Human Security and EU-Canada Relations Canadian Universities' Centre Berlin March 3, 2005 Wilfried von Bredow Institut für Politikwissenschaft Philipps-Universität D-35032 Marburg

makers in the research funding process and in R&D of security technologies to design security technologies in line with fundamental rights. These are the same all over the world. Although PRISE does not primarily assess technologies that are applied in civil and/or (semi-)military use outside the EU, its findings may be applied elsewhere too.

It should definitely be in the European Union's "Enlightened self-interest" that basic human rights are fulfilled within the EU itself. For this reason a thorough discussion must be undertaken on whether specific security policy measures really raise the level of human security internally in the EU. Democratic principles like the fundamental rights of privacy or freedom of speech or the freedom of assembly, the division of power between legislation, executive and judicial powers need to be protected. Lowering the existing barriers may lead to societies with less democratic general conditions and no more security.

2.4.5 Dimensions of security

The level of security is not easy to quantify. It strongly depends on the normative orientations and values involved. In any event, we have to deal with the problem of the proportionality of the measures. This proportionality may on the one hand be achieved by doing minimum harm to fundamental rights, but on the other hand a higher level of intrusion may be acceptable if the security gain is correspondingly higher. Thus the assessment of the potential security gains through the use of a specific technology is a prerequisite to a holistic proportionality assessment.

To circumvent the problems with the vague term "security", the scientific discussion focuses more on concepts like "risk", "uncertainty" and "danger". The following table shows the different concepts and their main attributes.

	Assessable	Not assessable
Can be influenced	Risk	Vabanque[45]
Given	Uncertainty	Danger

Table 2: Concepts of risk, uncertainty and danger

The security discourse nowadays focuses on "dangers" like terrorist attacks, industrial accidents and other non-assessable threats. It is not possible to conduct a classical risk assessment with regard to these issues, and the risk formula from the field of insurance mathematics (amount of loss x probability of occurrence) is no longer usable in this context as it is not possible to assess the probability of the occurrence of an event or to quantify the potential damage in monetary terms (ÖAW 2005, 30). Furthermore, partly calculated risks cannot be simply added because the overall risk to the system may be higher than the sum of the parts.

When looking at societal security it is necessary to accept that security and risk are socially constructed terms[46] which are influenced by far more than "objective" threats. It seems to be

[45] German term for a very risky game, where you wager all or nothing.

much more important how directly affected people are, how easily they can influence things and much less how high the probability of occurrence is. (ÖAW 2005)

In spite of these problems PRISE tries to deal with a potential security gain from security technologies. In order to be able to do so we differentiate between various dimensions of security.

Security of what?

In recent security policy discourse the main perceived threats are terrorism, organised crime and random crime. In order to assess security gain by using specific security technologies it is necessary to determine the extent to which the respective technologies or measures help to solve problems in the above mentioned areas.

Security for whom?

The PRISE project takes into account the two sides of security of individuals within a society. We will not look at national (state) security with its foreign policy and military approach. Instead we look at the security of the individual in society. This is supposed to be more than being protected against enemies from abroad. It also covers security from crime and terrorism as well as from intrusion into fundamental rights by public authorities or private entities. In the assessment of the potential security gain, it will also be necessary to show how a particular technology has built-in barriers against misuse by end-users whether public authorities, private enterprises or criminals.

Relationship of security in terms of prevention and prosecution

In the assessment of a potential security gain it makes a difference whether a technology is used for preventive measures or for the prosecution of suspects after a crime or terrorist attack has been committed.

Prevention is the main goal of modern security policy. The shift from a reactive to a proactive security policy that means dealing with unspecific risks rather than with specific threats is a radical turn in US security policy (Daase 2002, p.113)[47] and similar developments can be seen in Europe. Prevention deals with investigation, surveillance and proactive dataveillance. The new approach seeks to gather as much information as possible from different sources to sketch a picture of potential futures, in order to be able to anticipate the actions of suspicious groups and individuals. Successful prevention means detecting potentially threatening individuals or groups before they can carry out their planned attacks. This would be a real security gain for society. The most striking problem with prevention is reflected in the fact that as long as potential terrorists hide themselves by living “normal lives” they cannot easily be detected.

In contrast, reactive (inner) security policy is the policing and prosecution of suspects who have already committed a crime. In these cases new technologies may help to detect suspects, but the security gain is not as high. The negative effects of an attack have already happened. An effect on future security may be caused by deterrence, which may prevent other individuals

---

[46] See Daase et al (2002,25): Ch. Daase, S. Feske, i. Peters (2002): Internationale Risikopolitik – der Umgang mit neuen Gefahren in den internationalen Beziehungen, Baden-Baden

[47] Ch. Daase 2002, Terrorismus: Der Wandel von einer reaktiven zu einer proaktiven Sicherheitspolitik der US nach dem 11. September 2001 in: Daase et al. 2002 Internationale Risikopolitik, Baden-Baden

from committing a crime. What might be true for general criminality may not be so for politically or religious induced fanaticism and its consequences.

2.4.6 Can security be measured?

There are two different perceptions of security. The "objective security of a society" can easily be assessed by reading statistics on committed crimes and terrorist attacks. How effective security policies are can be seen from changes in statistics over time. However, it is not possible to draw conclusions about causality for a specific technology and its implementation.

Media, politics and the actual living context of members of society socially construct security as a perceived status of a group/state as well as of the individual[48]. It is very difficult to determine the "subjective feeling of security". It is however possible to obtain an insight into what people think by means of surveys and similar tools. At the same time it is astonishing that socially constructed feelings of insecurity, which are shaped by a multiplicity of parameters, can be re-shaped by monocausal technological approaches. The question remains: How can technology influence the discourse on perceived security?

A methodological problem arises with regard to the measurement of security: How can we measure the non-occurrence of an event? How many acts of terrorism have been prevented since 2001? How many could have been prevented by traditional means or technologies? The only thing we can do is to measure the quantity of incidents. The main problem remains: it is only possible ex-post. The ex-ante assessment of a potential security gain will be restricted to a plausibility check for the line of argumentation, and it will be necessary to look for best practice examples and try to assess the effectiveness of the measure (technical and organisational).

2.4.7 Conclusions

As shown above, security is a multifaceted phenomenon with at least two dimensions. It is individual security and it is societal (national) security. Neither is possible without the other. In this chapter we have shown that the focus between these two sides has shifted over time. In Section 2.4 we argued that the underlying problem is a trade-off between two dimensions of security rather than a trade-off between security and the fundamental right to privacy. It is the task of policy as well as of the citizens to find a balance between the security of the individual and national security. Without security policies and law enforcement we may face anarchy in both foreign policy and internal affairs. Without individual freedom and autonomy, democracy itself is threatened.

The proportionality of measures is the key for acceptance[49]. The proportionality of measures may be seen from two sides. Firstly it is the least necessary infringement, the least invasive measure to be taken in order to minimise the infringement of fundamental rights. In PRISE we give advice on how to do so and how to build that into security technology[50]. Secondly,

---

[48] For details see: J. Erikson and G. Giacomello (2007) (Eds.): International Relations and Security in the Digital Age, London/NewYork

[49] Again stressed by the European Parliament see: European Parliament resolution of 12 December 2007 on the fight against terrorism, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0612+0+DOC+XML+V0//EN Site visited 15th December 2007

[50] See D3.3 Design Proposals and the following chapters of this report.

proportionality may also be found in security gain. The more security you can gain from a measure the more it will be acceptable to infringe fundamental rights. The problem we are facing is that the security gain is not easy to calculate and is furthermore of different values to different people. Although there are figures on "objective security", like the number of attacks or of victims of attacks etc. there is a considerable problem in the legitimisation of measures and technologies. The difference can only be measured as compared with an equivalent period of time in the past – it is an ex-post statement. Even though a causality may be found between that difference and the measure or technology used, it can never be proven that an incident could not also have happened in an alternative scenario.

"Subjective security perception" is an important dimension of the issue. Because security is not something objective, many different influences may construct the feeling of security. One of these influences could be short-term focussed and non-proportionate measures. In that sense the implementation and use of security technologies may – despite their lack of an objective and measurable potential to contribute to a security gain – be an instrument to raise the level of perceived societal security. For the time being the main problem for the protection of fundamental rights is not a threat from a clear enemy, it is the lack of awareness of how privacy is affected by society's reaction to perceived risks. It is necessary to stimulate awareness to both societal security as well as the challenges that result from meeting the threats to this security with different means and technologies. Or as Louis Brandeis put it: "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding."[51]

[51] http://en.wikiquote.org/wiki/Liberty

3 The PRISE Approach

The PRISE project aims at defining criteria for the privacy-friendly security technology research funded in Framework Programme 7. The PRISE Approach will show how privacy can be designed into security technologies and how privacy considerations can be operationalised in the research and development process and the deployment phase of a security product. The legal compliance of security technologies and the technical and organisational means of achieving it are a major focus in this report. In this respect it is necessary to describe the requirements that security technologies should meet in order to

- comply with a minimum baseline of privacy rights,
- comply with general privacy principles, and
- comply with requirements exceeding the codified privacy requirements (PETs – the step further).

PRISE also discusses what other dimensions should be taken into account when analysing a research proposal in the FP7 programme. Even if research that is planned and laid down in a security call proposal within FP7 as such complies with privacy requirements, a project may have to be rejected on the basis of an overall assessment of its (societal) implications. If a security technology cannot clearly facilitate any gain in (societal) security or might even reduce an individual's security (see Chapter 2), there must be strong reservations about granting funding, no matter whether the planned technology would be privacy compliant as such. Since an overall assessment of the ethical implications of the research thus covers a wider scope than merely a privacy assessment, the context sensitive trade-off between privacy and security must also be considered.

PRISE therefore suggests the application of a three level assessment of security research proposals submitted. This three level approach is also addressed by research consortia about to apply for FP7 funding, as the approach enables them to consider all privacy-relevant aspects of their intended research and to achieve a privacy-friendly solution. The PRISE Security Research Impact Assessment approach describes a methodology for the evaluation of the societal impact and legal compliance of a research proposal. The approach provides assistance in different phases of a research and development process:

- What are the questions that must be addressed when assessing the impact of security research during the application process (plan)?
- What criteria should a security research consortium consider in order to develop a legally compliant and socially acceptable technology (build)?
- How can we ensure that the subsequent user of a security technology will use the technology in the least infringing way (run)?

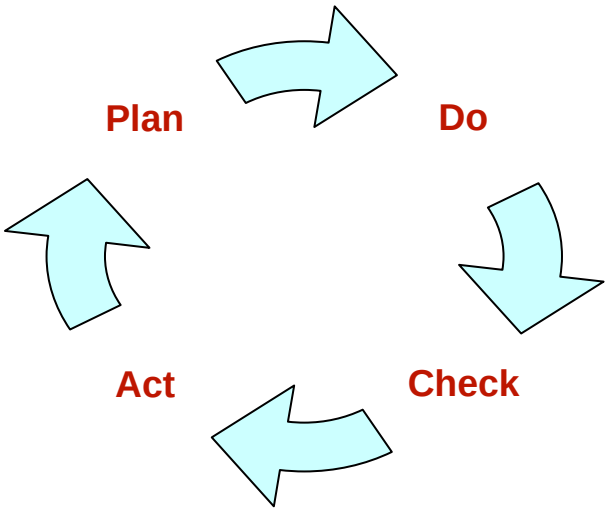

Figure 1: Process Life Circle

In a first step (3.1) we present the main findings of participatory events undertaken by PRISE in six European countries. The attitudes and arguments of about 160 citizens are of course not representative of the population but permit a very good insight into views on privacy and security and into the lines of argumentation prevailing in society. The main findings from these events are reflected in the three steps of the PRISE approach. The second step (3.2) presents the PRISE approach. It is basically a set of questions combined into a matrix to guide research project evaluation. A preliminary consortium – applying the PRISE Security Research Assessment – will be able to identify the privacy implications of future security technologies. The elaboration of the underlying PRISE concept and an understanding of how product and process related criteria are derived constitute the third step (3.3). Finally, practical instructions on the use of the matrix together with a comprehensive handbook listing possible tools to deal with identified privacy infringements are presented in a fourth step (Chapter 4).

3.1 The citizens have a say – input from the pTA events in 6 European countries

An important part of PRISE was to investigate attitudes and arguments of European citizens concerning privacy and security. In order to do so, the PRISE team, in collaboration with two contractors, organised interview meetings in the partner countries Austria, Denmark, Germany and Norway, as well as in Hungary and Spain. An interview meeting is a pTA (participatory Technology Assessment) procedure for gaining quantitative data from a questionnaire and qualitative data from group discussions.[52] The main results of the participatory events may be summarized as follows:

All the participants formulated some basic limits to the acceptability of privacy-infringing security technologies. An absolute limit of acceptance is the intimate sphere – especially the physical body. Technologies that intrude to the “very inner core” of privacy are unacceptable.

[52] Detailed description of the methodology and findings from the six countries may be found in D5.1 Questionnaire and interview guidelines and D5.8 Synthesis Report. More detailed data on the specific countries is published in the country reports D5.2-D5.7. All reports available from the PRISE website: http://prise.oeaw.ac.at/publications.htm

The threat of terrorism as such does not justify privacy infringements for most of the participating citizens. Interestingly, citizens are much more open to security measures for crime prevention. The participants also expressed their unease at the possibilities of security technology misuse. They strongly urged that misuse be prevented, but at the same did not believe that abuse can be prevented effectively. The participants were also concerned about function creep, where security technologies are used for purposes other than those intended.

Citizens also expressed their attitudes in positive ways, specifically on measures that make security technologies more acceptable. Most important is the proportionality between security gain and privacy loss. Proportionality is judged firstly according to efficiency – whether a security technology is able to increase security, and secondly according to the perceived level of threat that causes privacy infringements.

Trust in institutions is a key differentiating factor. Main measures to increase the acceptance of security technologies relate to the supervision of their use: Mandatory court orders before privacy infringing technologies are used and a strict control of individuals who handle such technologies were rated high by the participants.

Another conclusion was that privacy-infringing technologies should in any event be the last option. Participants strongly argued for using alternatives and non-technical measures to increase societal security. The vast majority requested that account be taken of democratic demands. For instance they wanted more public debate on the use of security technology, a debate that should involve both lay people and human rights organisations. Finally they called for compulsory Privacy Impact Assessments prior to the funding of research on and implementation of security technologies.

The PRISE approach incorporates these findings into the theoretical analysis on privacy and security and the existing know-how on deploying IT security measures and data protection management systems. Most of the conclusions from the interview meetings are therefore reflected in the PRISE three-step model.

The participants' clear objection to technologies that intrude the intimate sphere physically or mentally, together with considerations of fundamental human rights and dignity, lead to the demand for a Core Sphere or Baseline that must on no account be interfered with.

The strong emphasis on proportionality is reflected on the second level – Data Protection Compliance - as well as the third level – Context Sensitive Trade-off. Other demands made by the citizens are also taken into account in these levels: Prevention of misuse is part of the legal, organisational and technical terms within data protection management processes, which are tools for the data protection compliance part of the PRISE model. The insistence on court orders and the differentiated views of the threat of terrorism are incorporated on the third level – Context Sensitive Trade-off.

The following chapter describes the PRISE matrix in more detail.

3.2 PRISE criteria matrix

The PRISE criteria matrix's is the graphic manifestation of the PRISE model. It serves two purposes: Its first aim is to ensure that all aspects of relevance for the assessment of a security technology's impact on privacy are identified in a proposal. If these aspects are not addressed,

the matrix guides the user to legal, organisational and technical tools to overcome the privacy problems identified. After applying these tools it should be feasible to give an overall assessment of the potential privacy impact of the proposal concerned. Additionally recommendations may be needed for future users (e.g. recommendations on restricted use etc.)

The matrix is addressed to research and development (R&D) entities and preliminary consortia. At the same time the matrix is addressed to FP7 evaluators commissioned to evaluate proposals submitted for FP7 funding. The matrix can also serve as a guideline for them, ensuring that all relevant aspects are considered. In chapter 4 we present a short version of the matrix in two A4 forms to be used for proposal writers as well as evaluators.

	Criteria	**Tools**			**Warning Interim Status**	**Recommendations for…**		**Conclusions**
	Questions	**Legal**	**Organisational**	**Technical**	**Red/ Green Light**	**R&D**	**Users**	
Baseline								
Data protection compliance								
Context sensitive trade-off								

Table 3: The PRISE matrix

The matrix differentiates between three levels of analysis. A first step – the minimum or 'baseline' requirement of privacy protection – aims at assessing whether the technology allows for the collection or processing of intimate data (data about sex life, sexual preferences, intimate thoughts and conversations, conversations with oneself)[53]. Processing and collecting intimate data must be avoided in the first place (data minimisation) as it significantly increases the possibility of a lack of proportionality and legitimacy. Under German law, collecting and processing intimate data has even been ruled unconstitutional by the German Constitutional Court. Whether a technology's features and data processing are relevant in this context will be disclosed in the 'Criteria/Questions' column of the matrix. If relevance is identified, the matrix subsequently (in the next column) presents tools available to mitigate the relevant feature's impact on privacy. Not all the possible tools for achieving privacy compliance are merely technical measures. Nor do technical measures always exist to ensure compliance with all privacy principles identified[54] in Deliverable D3.2 Legal Report. Compliance requires a consideration of the organisational measures to be implemented by the subsequent user of the product. As an example, it is difficult to conceive of the technical enforcement of legitimacy and proportionality because they depend on the specific case and the rights affected (see D3.3 Proposal Report). Ensuring that the technology is used in a least infringing way, thus serving as the least intrusive means to achieve the legitimate purpose, requires consideration of the underlying investigation and the specific rights and obligations assigned to the data subject as well as the law enforcement or other public authority using the technology. This assessment

[53] Intimate data refer to the very inner circle of thoughts, communication and private life and are not the same as "sensitive data", used in the EU directive and respective national laws on data protection.

[54] General Privacy Principles are: Legitimacy, Purpose Binding, Proportionality, Transparency, Quality of the Data, Security of the Data.

cannot be mapped technically or designed into the technology as an automated function. The user must apply it on a case-by-case basis during every investigation and prior to each use of the technology.

Consequently, PRISE takes a broader approach. Organisational tools that back and support technical measures are also presented, as are legal tools, which are not in the hands of the R&D company or consortium. The tools listed in the matrix are not exhaustive but the matrix aims at listing the main tools. In addition to the matrix, more extensive references are found in the handbook (4.3), which elaborates on the listed tools and some additional ones. In the case of security technologies allowing the collection of intimate data, no tools mitigating this feature are presented, since a core sphere of individual privacy constitutes the limit of privacy, which must not be infringed even for the purpose of safeguarding security. However, the research consortium should assist the subsequent user of its technology by implanting features enabling the user to meet his legal duties such as the information rights of the data subjects.

If it is found that there are tools that can neutralise an identified privacy risk, a warning will show in the next column. If tools are available to achieve privacy compliance and the consortium plans to implement them, a green light is shown. Otherwise, a red light shows.

The questions that ensure that the consortium will consider all relevant aspects of its research and its impact on privacy comprise – broken down to the three levels described –:

Core Sphere:

- Does the proposed technology interfere with human dignity?
- Does the proposed technology interfere with persons' physical integrity?
- Does the proposal allow surveillance in homes (assumption: place of retreat and personal life-style; intimate sphere)?
- Does the proposed technology allow collection or processing of intimate data (data about sex life, sexual preferences, intimate thoughts and conversations, conversations with oneself)?
- Does the proposed technology allow interaction with partners like spouses, children, lawyers, or priests?

Data Protection Compliance:

- Does the technology lack a specification of the purpose of use and data collection or is the purpose stated very broadly?
- Does the possible technology use and data collection and processing require the adoption of a new legal basis?
- Is there a less intrusive means available that would achieve the intended result with comparable efficiency?
- Does the technology aim at or allow the collection of sensitive data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical persuasion)?
- Does the technology involve the linking of data, data merger or data analysis?
- Does the technology require removing anonymity of data subjects?
- Is the technology used regardless of whether the individual is suspected of any wrongdoing?
- Is lack of transparency regarding technology use (prior to and/or after use) the default setting?

Context-Sensitive Trade-Off:

- Does the proposed technology aggravate judicial scrutiny?
- Does the proposed technology facilitate societal security?
- Does the proposed technology aim at crime prevention?
- Does the proposed technology aim at prosecution?
- Is the main field of application combatting…
    - terrorism,
    - organised crime, or
    - random crime?
- Does the proposed technology increase individual security against …
    - the state (in terms of privacy protection) or
    - other spheres (economy, social)?

3.3 Basic Terms and Categorisation

Technologies typically run through certain phases of development and, once established as products on the market, through life cycles. In these phases, different stakeholders are responsible for privacy or data protection. Phases, their characteristics and the stakeholders involved that need to be taken into consideration are:

Development of technologies:

- Purpose of use and technical implementation is not readily defined.
- Stakeholders are public and private research organisations.

Development of products:

- Purpose of use and technical implementation is defined on the basis of the results of a market analysis.
- Stakeholders are mainly private enterprises.

Introduction of business or governmental procedures:

- Typically purpose is defined and means of implementation selected in two phases (plan and build phases according to the life-cycle model for procedures).

- Stakeholders are any type of organisation.

Operation of business or governmental procedures:

- Processes and supporting solutions (technology, hardware and software) are in place and maintained.
- Stakeholders are any type of organisation.

3.4 Introduction to Methodologies

Information security management and data protection management are closely interlinked. The linking elements are Articles 16 and 17 of EU Directive 1995/46/EC, laying down security safeguards for the processing of personal data within the scope of the Directive. Though the Directive for security procedures and the corresponding applications of the member states do not apply directly, national legislation following the legal principles of Directive 1995/46/EC is in place in many member countries.

In the context of information security, good practice is well established and in many cases has led to a number of ISO standards. These standards follow a structure that is also well applicable to the planning, implementation (building), operation and auditing of organisational and technical data protection measures. The main difference between security standards and data protection standards is their target – while security aims at the appropriate level of confidentiality, integrity and availability (CIA), data protection aims at the implementation of the relevant data protection legislation laying down specific requirements to be met by the data controller. These requirements can roughly be summarised in a number of data protection principles, such as legitimacy, purpose binding, proportionality, transparency and high quality and security of the data.[55]

In the context of PRISE work, a relevant overlap between IT security and data protection exists as follows:

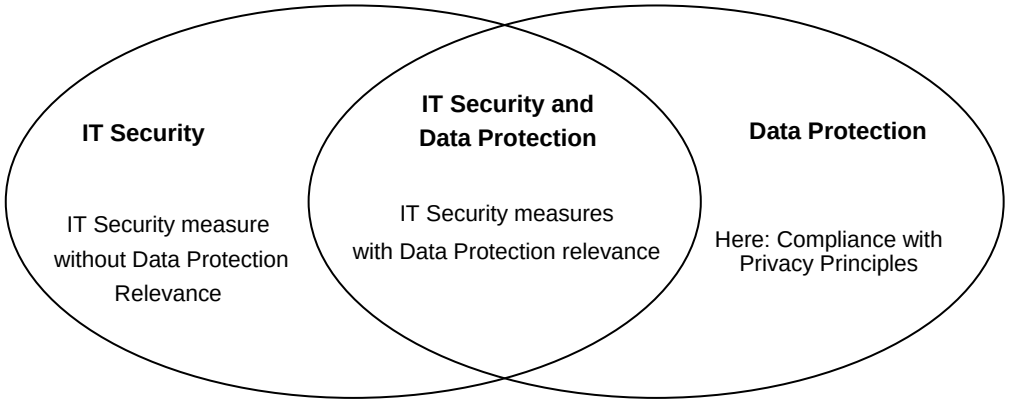

Figure 2 Overlap between IT Security and Data Protection

[55] See D3.2, page 19.

Two of the identified privacy principles are also covered by IT Security. These are the principles 'Quality of Data' and 'Data Security'. Bearing in mind that IT Security aims at ensuring a high level of date confidentiality, integrity and availability, and that it uses technical and organisational means to achieve these aims, a similarity to the measures ensuring data security and quality of data is apparent. Directive 1995/46/EC explicitly states[56]:

"Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental loss, alteration, unauthorized access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

The German Data Protection Act provides[57] for a more detailed description of what generic threats must be met by organisational and technical measures:

"Where personal data is processed or used automatically, the internal organisation of authorities or enterprises is to be arranged in such a way that it meets the specific requirements of data protection. In particular, measures suited to the type of personal data or data categories to be protected shall be taken

- to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used (access control),
- 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 it is possible to check and establish whether and by whom personal data has been input into data processing systems, modified or removed (input control),
- to ensure that, in the case of the contracted processing of personal data, the data is processed strictly in accordance with the instructions of the principal (job control),

---

[56] Article 17 of Directive 1995/46/EC.

[57] In the annex to Article 9 German Federal Data Protection Act. Available in English at http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf.

- to ensure that personal data is protected against accidental destruction or loss (availability control),

- to ensure that data collected for different purposes can be processed separately."

Many of the security technologies covered in D2.2 Technology Report involve electronic data processing. If these technologies are used to collect evidence which is to be used in a criminal trial, special emphasis must be placed on a complete chain of verification, proving that data has not been altered or was indeed collected from the suspect charged.[58]

Information security covers well-elaborated standards on a process and product level, like how to ensure data confidentiality, integrity and availability – and subsequently the security and quality of data. These standards will be used as a starting point for establishing a model for a generic data protection management process, which will cover organisational means, procedural means and criteria broken down to the specific products at the end of the research and development process.

In doing so, the existing standards will – after an initial description – be mapped to

- levels (organisation related, process related, or product related),

- implementation object, and

- addressee.

In order to make sure that a research project's final product (or prototype) is privacy compliant, a process-related guide on how to include considerations on privacy compliance into the research process is necessary. Furthermore, since the level of privacy impact of a security technology depends not only on the technical features of the technology, but also on the specific use in a specific case, this approach will also cover a process-related guide for users of security technologies on how to ensure a privacy compliant use.

This chapter will analyse good practice processes, methods and structures in organisations well established in the context of information security and map them with established, as well as emerging, processes, methods and structures for privacy and data protection.

3.5 Analysis of processes, methods and structures established in information security

In the context of information security good practice is well established. This covers products to be used in the context of security, and procedures for information security management in organisations. The following section will provide an overview of different standards in this sector as well as some more in-depth descriptions of selected standards.

[58] For example A. Geschonneck 'Computer-Forensik', 2006, (in German) is describing how to collect data from computers in a way that the data can be used as evidence at a court of law.

3.5.1 Product related approach

In the context of products based on predecessor criteria systems such as ITSEC[59] the **Common Criteria (CC)**[60] are established as ISO standard 15408. The Common Criteria provide a scheme of how to **describe and certify the security features of a product** based on an evaluation carried out by an independent third party.

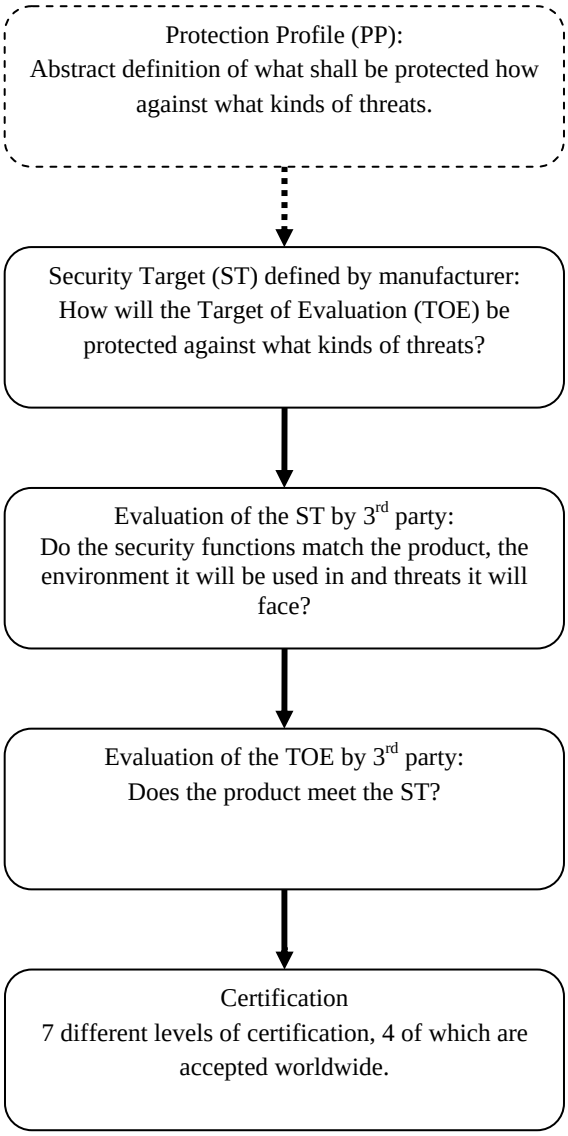

Figure 3: Common Criteria certification methodology

[59] See http://www.bsi.de/zertifiz/itkrit/itsec.htm

[60] Download e.g. via http://www.bsi.de/cc/index.htm

Core elements are security targets, corresponding security functions and their strength as defined and described by the issuer of the product. An independent certificate authority first evaluates the security target itself, i.e. whether the security functions match the product if they are implemented properly. This security target may be based on a protection profile which contains an abstract definition of an asset and its protection.[61] The actual product is evaluated in a second step, i.e. are the functions implemented properly? This two-step approach helps to eliminate security functions which do not actually raise the level of security.

A successful certification process ends with the product being certified on one of seven defined Evaluation Assurance Levels (EAL). Up to level 4 these evaluation assurances are accepted worldwide. The certification reports are published on the internet.[62]

3.5.2 Process and organisation related approaches

Guidelines on the planning, construction, operation and improvement of an **Information Security Management System (ISMS)** are standardised in ISO 27001. ISMS refer to roles and management functions in organisations as well as the processes needed for the information security management. How concrete the description of roles, functions and processes are may differ. ISO 27001 provides general guidelines for **roles and functions** and describes input and output for **processes** needed in the context of information security management, but does not describe good practice workflows in detail. Additional publications based on ISO 27001 provide examples of how roles and functions may be implemented properly in organisations and what a detailed core process could be like.[63]

Methods related to ISMS are also standardised. This standardisation is mainly focused on methods for **risk assessment** (ISO TR 13335, e.g. basic assessment and the baseline approach). Supporting catalogues of control objectives and controls (ISO 17799 / 27002) and the baseline protection catalogues[64] published by the German Federal Office for Information Security (BSI) are available for these different methods. These catalogues contain a collection of good practice organisational and technical security measures that are partly abstract (mostly ISO 17799 / 27002) and partly very concrete on a technical instruction level (especially technical measures in the baseline protection catalogues).

The baseline protection methodology and other standards developed by the German Federal Office for Information Security (BSI) are such publications.[65] As it provides a comprehensive process-oriented framework for implementing IT security measures, it will be discussed in greater detail to show how the rather abstract definitions of ISO 27001 can be put to use in practice.

---

[61] There is also a separate evaluation scheme for protection profiles, see http://www.commoncriteriaportal.org/public/developer/index.php?menu=8

[62] Available at: http://www.commoncriteriaportal.org/public/consumer/index.php?menu=5

[63] See for example the standards issued by the German Office for Information Security (BSI), http://www.bsi.de/literat/bsi_standard/index.htm

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

[65] See http://www.bsi.de/literat/bsi_standard/index.htm

In the context of the BSI's baseline protection methodology, the units of analysis are "IT assets". This term "refers to all the infrastructural, organisational, personnel and technical components which assist with the performance of tasks in a particular area in which information processing is applied."[66] It can apply to the whole organisation of e.g. a government agency, but also on a smaller scale, for example only concerning one small administrational division.

The starting point is an analysis of the relevant IT infrastructure. This means creating a network plan containing all the IT systems linked in the network (PCs, switches, servers etc.) as well as information on the internal network links themselves (e.g. LAN connections and backbone technologies) and information on connections to the outside world (e.g. dial-up access, radio links etc.). Information on their location is also needed, as this is relevant in terms of IT security, e.g. restricted access to server rooms. In a second version, identical components with the same protection requirements are grouped to reduce the plan's complexity; an example would be grouping identical client PCs running the same software and used for the same tasks.

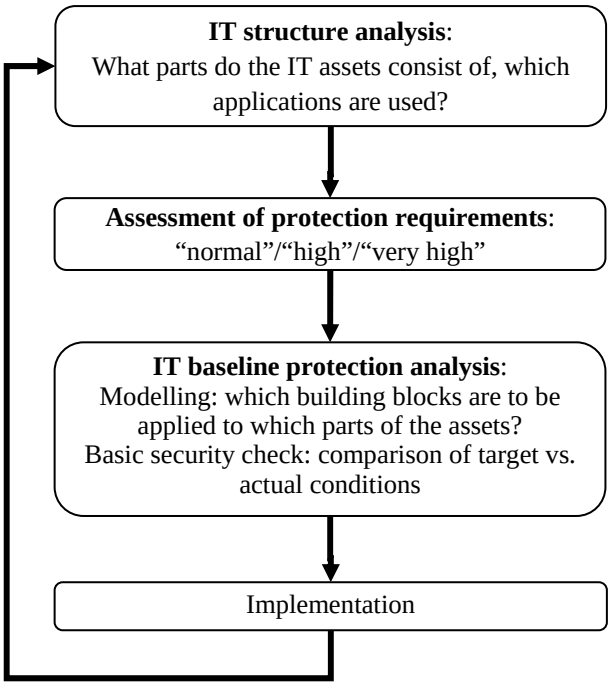

Figure 4: BSI Baseline Approach

The next step is to assess the protection requirements. There are three different levels, based on the impact a violation of the three aims of IT security (see above) would have on the organisation operating the IT assets. The three levels are "normal", meaning that consequences

[66] See http://www.bsi.de/english/publications/bsi_standards/standard_1002_e.pdf ,28

are limited, "high", meaning possibly grave consequences and "very high", meaning that a failure of the IT assets in question would pose an existential threat to the organisation. Typical damage scenarios would be violations of contracts or laws, bodily harm, financial consequences or a negative impact on fulfilling assigned tasks. As such setbacks are hard (if not impossible) to estimate ex ante, the definition of the protection levels is only qualitative and not quantitative. Due to the "maximum principle" employed in assessing them, it is sufficient for one part of the system to be classified as "high" or "very high", in order for the whole system to be given the same classification. An example would be a computer used for wage and salary administration. Whereas a day or two of downtime could be dealt with (i.e. protection requirement "normal" in terms of availability), illegal disclosure of such data could have far worse consequences (i.e. protection requirement "high" concerning confidentiality). Therefore, the protection requirement for this computer would be "high".

After the appropriate protection requirement has been determined, security safeguards have to be considered. The baseline protection catalogues offer a modularised framework of building blocks addressing different issues. They are organised in five "layers", dealing with general aspects of IT security, security of the infrastructure, security of the IT systems, network security and security at application level, respectively. Each of these "layers" includes a number of blocks dealing with specific questions. To give an example, the application layer includes guidelines for specific frequently used software programs. There is also – as a part of the first layer – a block dealing with data protection. These blocks each include an enumeration of threats to the specific object, as well as standard safeguards to address them. These threats[67] and safeguards[68] are explained in more detail in separate documents. The threat catalogue contains information on threats ranging from lightning and blackouts to insecure encryption and employees writing down their passwords in order not to forget them. The safeguard catalogue describes good practice standards for addressing threats.

The next step is to relate the findings gained from analysing the IT structure to the different blocks. This process is called "modelling" and results in a model of the IT assets in which the blocks and the different components of the IT assets are linked. Components which cannot be modelled appropriately are to be singled out for further analysis, for example using risk assessment technologies. The result provides an overview of the assets complete with security issues to be addressed and ways of doing so.

If the protection level needed is "normal", then the standard safeguards from the catalogues are normally sufficient. For the protection level "high", additional safeguards tailored to the specific IT assets may have to be developed. If the protection level needed is "very high", then the measures included in the BSI's catalogues are usually not sufficient and developing such extra measures is necessary in most cases. The BSI supplies a risk assessment method based on its baseline protection catalogues for this.[69]

Once it has been established how the IT assets ought to be protected, the next step is to compare "is" and "ought". If existing IT assets are to be evaluated, this takes the form of a check of whether the measures stipulated by the safeguard catalogue are implemented. If not, an implementation plan for them has to be devised. As these methods can also be applied to IT

[67] See http://www.bsi.de/english/gshb/manual/download/threat-catalogue.pdf
[68] See http://www.bsi.de/english/gshb/manual/download/safeguard-catalogue.pdf
[69] See http://www.bsi.de/literat/bsi_standard/standard_1003.pdf

assets which are only in the planning stage, it can also take the form of a development plan. However, usually a combination of the two is to be found. If this check finds that necessary measures are missing, they are to be implemented.

There is a **certification scheme** based on the BSI's baseline approach.[70] ISO 27001 also provides a certification scheme for organisations. Currently more than 3600 certificates have been issued under the latter, mainly for organisations in the private sector.[71]

The standards ISO TR 13335, ISO 17799 / 27002 all have a somewhat flexible area of application. They may be applied for a central management system of an **organisation** or more focused on a business or governmental **procedure, the related organisational divisions and related IT infrastructure**.

Outside the ISO standards a number of additional supporting methods for the risk assessment are available, especially Failure Impact Analysis (FIA) and Attack Tree Analysis (ATA). Failure Impact Analysis (FIA)[72] focuses on components as Component Failure Impact Analysis (CFIA) in the context of the IT Infrastructure Library (ITIL), a good practice process framework for IT Service Management (ITSM)[73]. CFIA is used to support optimisation availability management and service level management, two important processes in the ITIL process framework.

Attack Tree Analysis was introduced by Bruce Schneier in 1999[74] and allows the analysis and evaluation of attack vectors for new procedures, related systems and applications. In the context of a broader **Technology Assessment and Technology Impact Assessment (TIA)** Attack Tree Analysis can be applied to generic technical implementation models, e.g. schemes of building blocks to implement the technology.

3.6 Transfer of the findings to privacy and data protection

The approaches described for information security have largely been transferred to privacy and data protection as well. Standardisation is not as advanced as with information security, since the interpretation of privacy and data protection and consequently the corresponding legislation differ substantially worldwide. Standardisation on a European level is led by the European Committee for Standardization (CEN). CEN has issued a number of CEN Workshop Agreements (CWAs) with regard to the standardisation of data protection and privacy practices. CWAs 15499-1 and -2 describe a Personal Data Protection Audit Framework.[75]

---

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

[71] See http://www.iso27001certificates.com/

[72] See for example http://www.mnm-team.org/pub/Publikationen/hss05c/PDF-Version/hss05c.pdf

[73] For further information on ITIL see http://www.ogc.gov.uk/guidance_itil.asp

[74] Schneier, B., Attack Trees, Dr. Dobbs Journal, December 1999.
Download: http://www.schneier.com/paper-attacktrees-ddj-ft.html

[75] Available for download at http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cen+workshop+agreements/dppcwa.asp.

As described earlier, European Directive 95/46/EC provides a common ground for Europe. The following text contains a short description of various approaches and a more in-depth description of the Privacy Seal issued by ULD[76].

Privacy Impact Assessment (PIA)[77] was introduced by Roger Clarke in 1996 as part of the Technology Impact Assessment. PIA may be used to assess the potential privacy impact of new technologies on society based on privacy or data protection principles in a general way. PIA today is widely established in Canada[78], the United States[79], Australia[80] and the United Kingdom[81]. As a result, potential privacy risks become visible and countermeasures such as the use of **Privacy Enhancing Technologies (PETs)** or regulation by law to limit areas or ways of application may be suggested. Depending on the principles used, the results of this assessment may differ. In addition to the data protection principles extracted from the European Data Protection Directive 1995/46/EC[82] the **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** [83] or the **Fair Information Principles**, based on the "Records, Computers and the Rights of Citizens" report by the U.S. Department of Health, Education and Welfare[84] may be used.

Applied to products, the PIA may be carried out as a compliance analysis on a legal and technical level with respect to national privacy or data protection legislation. Another way is to integrate such an analysis into the development process. Solving problems related to privacy concerns is both easier and cheaper at this stage than when the product is finished. In this way a **privacy preserving design and the integration of Privacy Enhancing Technologies (PETs)** are possible. First certification schemes are available for assessing privacy compliance of products and services.[85] These schemes provide a set of criteria based on data protection legislation against which an independent third party evaluates an already developed product.

3.6.1 Privacy Seal

An example of a certification scheme is the Privacy Seal issued by ULD.[86] Its criteria are described in a catalogue of questions consisting of four sections, which will be described below.[87]

---

[76] The ULD Privacy Seal is currently the only existing product related privacy certification scheme issued by a supervisory authority.

[77] See http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html#App , and http://www.anu.edu.au/people/Roger.Clarke/DV/PIAsFlaherty.html

[78] See Privacy Commissioner of Canada: "Privacy Impact Assessment" at http://www.privcom.gc.ca/pia-efvp/index_e.asp

[79] See Department of Homeland Security's Privacy Office – Privacy Impact Assessment at http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm

[80] See Privacy Commissioner of Australia: "PIA Guide" at http://www.privacy.gov.au/publications/pia06/index.html

[81] See Information Commissioner's PIA Handbook at http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

[82] See Deliverable D3.2. page 16.

[83] See http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[84] See e.g. http://www.privacyrights.org/ar/fairinfo.htm

[85] E.g.: a privacy seal issued by the Privacy Commission of the Federal Land of Schleswig-Holstein in Germany, see https://www.datenschutzzentrum.de/guetesiegel/index.htm and the Federal Land of Bremen in Germany, see http://www.datenschutz-bremen.de/audit.php.

[86] See https://www.datenschutzzentrum.de/guetesiegel/index.htm and the seal issued in the Federal Land of Bremen in Germany, see http://www.datenschutz-bremen.de/audit.php

[87] The following paragraphs are all based on Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH, available at: https://www.datenschutzzentrum.de/download/anford.pdf

Fundamental design questions

The first section deals with fundamental design questions of the product. Three criteria are important here, all of which are seen as PETs. The first criterion is data avoidance. The idea behind it is that data that is not being collected in the first place enjoys the best protection. This stage asks whether measures to avoid the collection of personal data are implemented and, if collecting such data is inevitable, whether the amount of data is minimised. The second criterion is if it is possible for the data subjects to act anonymously or pseudonymously. Important questions are whether personal data is deleted or at least anonymised at the earliest date possible, and what is done with unsolicited personal data received. The third criterion is transparency, which refers to the data processing itself as well as to the product's documentation. The latter has to be exhaustive, up-to-date and understandable for both data processors and data subjects in order to make the processing transparent.

Legitimacy of the data processing

The second section scrutinises the legitimacy of the data processing. According to German data protection law, data processing requires either a statutory provision legalising it or the consent of the data subject. These are the main questions asked in this section. Concerning the statutory provisions, the relevant legislation is searched to determine whether it allows the proposed data processing and if it imposes additional safeguards or restrictions, for example concerning sensitive data. Relevant legislation includes the Federal Data Protection Act as well as those of the *Laender* and other laws relevant in the context of the specific product, e.g. police or school laws. The requirement of the consent of the data subject includes asking whether there are forms for obtaining consent, how they are designed and whether they contain the necessary information (i.e. what kinds of data are processed for which purposes, whom are they transmitted to, is it clear that consent can be denied, are disadvantages associated with refusing consent?). It is also asked whether consent is really voluntary and how refusal is processed (e.g. refusing permission for personal data to be forwarded to other companies for promotional use).

Technical and organisational measures

This section is most closely related to IT security. It focuses on measures to prevent the data from being unlawfully accessed, changed, disclosed or otherwise abused. In this section, questions are on a very technical level.

Specific questions asked include how access to the physical data storage is denied to unauthorised persons, as well as how authorisation procedures are handled in data processing. This refers, among other things, to password protection and its secure implementation (e.g. do passwords expire after a certain time, is there a minimum length required, are there restrictions on their reusability?) or other access control measures such as chip cards or biometrics (which may themselves be subject to data protection legislation). Role-management is also important. This means that different roles and their respective competences are defined and applied. An example would be the separation of data processing and system administration profiles on PCs – a normal user must not be able to change the system's configuration whereas an administrator does not need access to personal data being processed – and again, not every data processor needs access to all personal data. Other measures dealing with denying unauthorised access would be firewalls, intrusion detection systems, anti-virus software and encryption. Here, the link to information security is especially obvious. Since not every unlawful data disclosure or altering is done intentionally, measures against unintentional disclosure, for example by negligence or accident, have to be considered as well. Examples would be

removing information about the author added to documents by text-processing software by default or reducing the viewing angle of monitors to prevent others from spying on them. The general requirement of transparency is to be ensured by logging the data processing (where mandated by law), which means keeping records of who processed the data in which way at what point of time. However, another issue arises with logging: The log files themselves can be problematic from a data protection perspective, since they contain personal data and may allow surveillance of the employees. Therefore, these logging processes are subject to a specific check which uses many of the criteria outlined for the general certification procedure, including data avoidance and transparency.

Special requirements are also listed for some specific technologies, such as CCTV and chip cards, since the German Federal Data Protection Act contains special provisions regarding these technologies. They include disclosing that data is being collected, for example by putting up signs stating that the area is being watched via CCTV.

The rights of the data subject

The rights of the data subjects are the topic of the fourth section. The first question here is how the data subject is informed that his or her personal data is processed, for example using automated notification procedures comparable to itemised bills for telecommunication. The second question refers to how inquiries filed by the data subject are handled. Automated procedures that reduce delays in answering inquiries as well as the inhibition level are a plus here, though the question of how the person filing the inquiry is authenticated must also be addressed. Another question is whether the information given is complete (i.e. stored data, the purpose it is used for, legal basis, origin and recipients of data, logical structure of automatic procedures if used). The next point concerns correcting, deleting and blocking (i.e. not deleting, but barring from further processing) data. It is asked how such requests are handled (e.g. automated correction methods), whether data deleted is really deleted irreversibly (how is it done, what is done with backups and data forwarded to other organisations?) and how the blocking of data is handled. The last issues addressed in this section are objections to processing and counter-statements. How is it ensured that objections are processed, and are they forwarded to the 3rd parties to whom the data has been forwarded? How are counter-statements included in the data?

Based upon these criteria, an accredited expert[88] drafts a certification report which is then forwarded to ULD, where it is double-checked. Certified products are listed on the ULD website, together with a short version of the report.[89] The seal issued is valid for two years; if the product remains unchanged a simplified recertification is possible. During a public tender process public authorities of the Land of Schleswig-Holstein must prefer sealed products over such which are not sealed.

[88] As the certification process encompasses both technical and legal dimensions, separate accreditations are given for the two fields. An expert can, but need not, be accredited for both fields. However, a positive report on both fields is needed for the product to be certified.

[89] See: https://www.datenschutzzentrum.de/guetesiegel/register.htm

So far, such certification schemes are only available on a regional level.[90] The project **EuroPriSe**, which aims at establishing a European privacy seal, has been started recently as a part of the eTEN programme.[91]

With respect to business or governmental procedures and organisations, the privacy or data protection legislation provides a framework for a privacy or data protection management system, though this term is not established as such yet. Legislation includes roles and functions in the context of data protection management (e.g. Privacy Commissioners or Data Protection Advisors) and describes input and output for processes (e.g. the maintenance of an inventory of procedures in which personal data is processed). Additionally, a workflow oriented good practice data protection management process model optimised for the use together with the baseline protection information security management process model has been introduced for organisations.[92]

In the context of governmental procedures audit schemes based on national data protection legislation are in place.[93] For enterprises the "quid!" audit scheme was developed in Germany based on a private initiative.[94] This scheme covers data protection management of (private) organisations.

3.7 Criteria for privacy compliant security technologies

The aforementioned approaches and standards can be applied to and synthesised for the context of security research and security technologies. It is evident that such an approach embraces product and process related criteria of a technical and organisational nature.

3.7.1 Implication of Articles 13 et al. of Directive 1995/46/EC?

Before further elaborating these PRISE criteria, it is necessary to take a closer look at the addressees involved in the research and development and use of security technologies. It must be discussed if and to what extent there is an obligation to comply with the privacy principles and to produce security technologies compliant with the privacy principles described in D3.2 Legal Report (see footnote 28). Article 13 of Directive 1995/46/EC states:

"Member States may adopt legislative measures to restrict measures to restrict the scope of the obligation and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, […]."

---

[90] See above, footnote 22

[91] See http://www.european-privacy-seal.eu/ and Bock, K., 'EuroPriSe – Das Datenschutz-Gütesiegel aus Schleswig-Holstein wird europäisch', *Datenschutz und Datensicherheit* 6/2007, 410, Wiesbaden 2007.

[92] Meints, M., 'Datenschutz durch Prozesse', *Datenschutz und Datensicherheit* 2/2007, pp. 91-95, Wiesbaden 2007. And: measure 7.1 in the chapter 1.5 "Data Protection" of the baseline protection catalogues, http://www.lfd.m-v.de/dschutz/informat/grunschutz/B1_5_Datenschutz.pdf

[93] For example in Germany: Datenschutz-Behördenaudit of the Federal Land of Schleswig-Holstein (see https://www.datenschutzzentrum.de/audit/index.htm) and the audit scheme of the Federal Land of Bremen (see http://www.datenschutz-bremen.de/audit.php)

[94] See http://www.tuvit.de/47365.asp.

At first glance this provision could be seen as an exemption allowing restrictions of privacy and thus also security technologies which disregard or infringe privacy. Yet, such an interpretation of Article 13 is not correct. The provision allows for the adoption of regulations which restrict privacy. It takes effect only on a regulatory level and allows for the national law makers to pass laws in the context of law enforcement, national security and public security. Measures in these areas are usually addressed at or involve investigation or intelligence about citizens, and thus the processing of personal data. Article 13 does not include a proposition on technical features of technologies which are used to carry out the powers of investigation etc. which were passed following the exemption in Article 13.

As described before, the level of privacy impact of security technologies results from different determining factors:

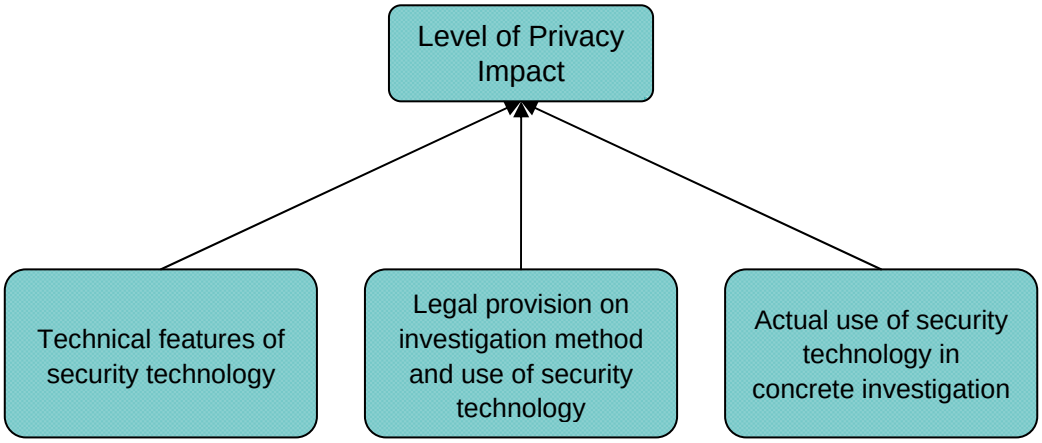

Figure 5: Factors determining level of privacy impact

If Article 13 merely contains an authorisation to adopt national laws which restrict privacy, are there reasons why companies doing research and development of security technologies should consider or have to comply with privacy principles?

Looking at Directive 1995/46/EC, Articles 3, 4, and 2 specify the addressee of the provisions laid down in the data protection directive. All the obligations described in the directive are addressed at data controllers or their processors[95]. These are the entities which determine the purposes and means of processing. As the development of security technologies covers the processing of personal data only as far as management of the project is concerned, project partners which engage in security technology research and development are directly bound by the Directive (more specifically: its national implementation law) if personal data is processed in the project. The Directive does not contain a provision directly binding entities which develop systems or technologies, which are later used by controllers or processors. Even

[95] Definition in Article 2 (d) and (e).

though the technical features of a security technology can increase or reduce the level of privacy impact, the Directive does not address the development of technologies used for the processing of personal data.

Yet, even if not legally bound directly by European privacy law, developers of security technologies do have to put a main emphasis of their research and development efforts on compliance with privacy law:

Any research company or project which does not consider the legal obligations of their subsequent buyer will produce a product which is not marketable. Privacy compliance is however often regarded as a non-functional requirement by developers of products and services. A balancing of all non-functional requirements is carried out when deciding about the functionality. As long as no explicit demand for privacy enhancing products dominates the market (market demand as a driver) or a legal obligation for developers of data processing technologies to develop privacy compliant products is introduced (law as a driver - developers as addressees of the privacy directive 1995/46/EC) this balancing of all non-functional requirements may well result in a company's decision to not implement all features which would ensure privacy compliance.[96]

A generic research and development process comprises several steps such as a market analysis, the definition of functionality, product development and testing looks as follows:

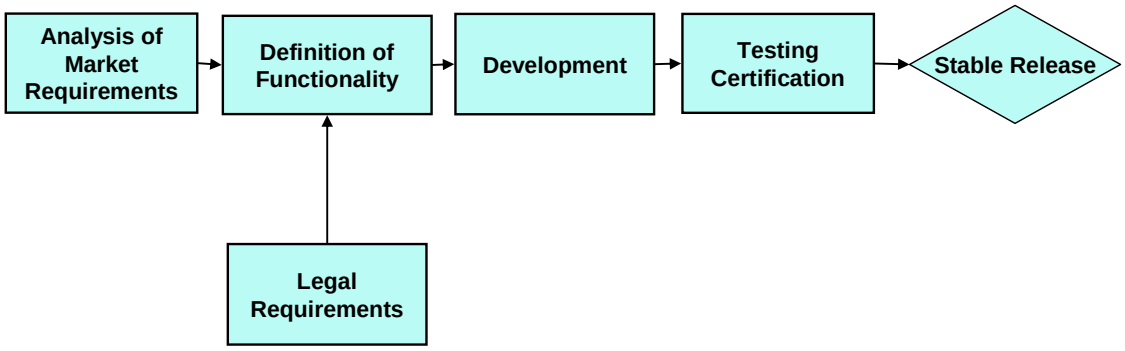

Figure 6: Generic research and development process

Before defining the functionality of the product, a market analysis is usually carried out. This includes an analysis of the target group and an analysis of the legal obligations, technical requirements, and standards which must be considered. If the subsequent purchaser of a security technology is bound by legal provisions concerning compliance with privacy law, the product must be designed in a way that makes it possible for the subsequent user to meet his obligations when applying the technology. Otherwise a potential buyer would have to refrain from buying the product.

[96] A presentation on the product design process and the consideration of functional and non-functional requirements at SAP was given by S. Paulus on the PRISE final conference. See http://prise.oeaw.ac.at/docs/conf_docs/28/Paulus-Implementing_Privacy_Criteria-20080429.pdf.

A general problem when analysing the legal obligations could be seen in the diverse national privacy laws in Europe. Nevertheless, the Data Protection Directive forms the common ground for all national privacy laws, and for this reason developing companies and projects can consider the privacy principles as a minimum privacy standard.

A closer analysis of who could possibly buy the security technology which is to be developed reveals two generic buyers:

- public authorities, governments, states, or / and
- private companies such as security companies providing personal protection or detectives.

The European Commission has emphasised that it supports dual use approaches of research in the FP7 funding scheme.

The legal obligations of these two generic organisations when using security technologies and thereby processing personal data as controllers can be described as follows:

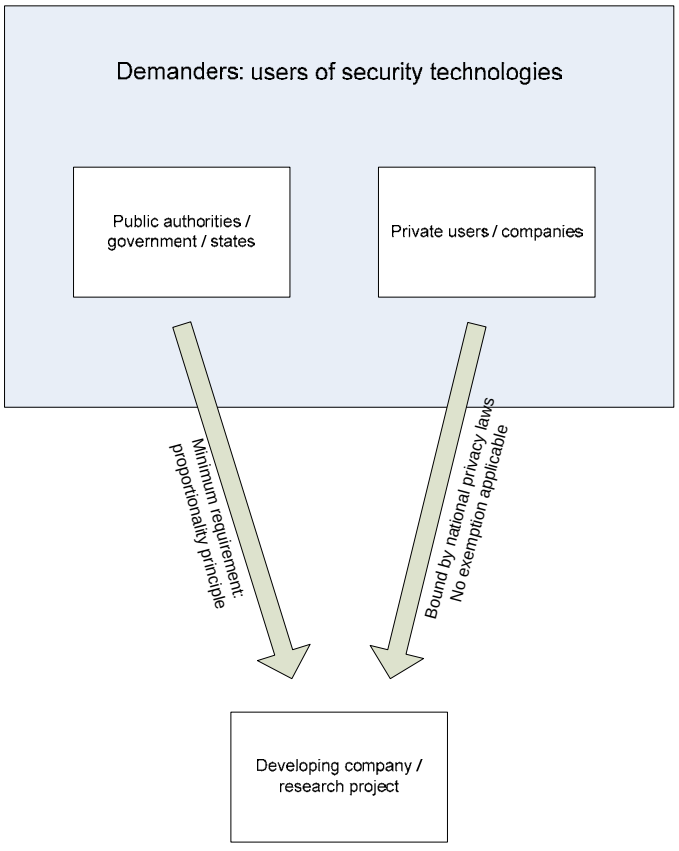

Figure 7: Market analysis: security technology demanders' obligations

3.7.2 Legal obligations of private security product users

Whenever dual use of a security product or technology[97] is intended or possible, the developer of such a product has to consider the legal obligations of private data controllers using the product. Any use of security technology involving the collection or processing of personal data falls under the Data Protection Directive or its national implementation legislation.

The Data Protection Directive is addressed to data controllers, as described above. Any legislation restricting privacy which is adopted in line with the authorisation of Article 13 of the Directive is addressed to public authorities (police, intelligence services), since these organisations are responsible for safeguarding national security, public security and law enforcement. The corresponding provisions are not applicable to private organisations.

Private organisations using security technologies for legitimate purposes have to comply with all the data protection principles described in D3.2. There are no exemptions to this general obligation of data controllers.

Consequently, security products which are to be used by private users must permit compliance with the data protection principles. This means that the technical features of the product must be designed in a way that, for example, permits transparent and purpose bound use. For an in-depth description of criteria, see 4.3.

3.7.3 Legal obligations of public security product users

The situation is different for public authorities using security products under specific regulations, for example when carrying out investigative powers assigned by law. Depending on the specific national legislation allowing the intended use and depending on the actual use in a specific case, privacy principles may be restricted. For example, during a covert investigation there is usually no room for transparency. As this principle cannot be upheld if the purpose of a covert investigation is not to be thwarted, transparency is usually provided for after the investigation has ended, for example by means of notification obligations. However, if the product has not been developed to be used under only one specific national regulation, which could permit the assessment of possible restrictions to future use resulting from privacy principles, and if instead the developer targets buyers from different countries, the product must allow compliance with data protection principles generally. It is not possible to assess the impact of all possible national legislations covering the possible future use of the product, and the developer might indeed lose possible customers if the final product cannot be used in accordance with the specific national legislation. Whether a restriction of certain privacy principles will apply is a decision made at national legislative level.

Furthermore, a second consideration has to be taken into account. Whenever a fundamental right like privacy is restricted, the requirement of proportionality of the restriction must be satisfied. There is never an exemption to this principle, yet depending on the specific case of use either privacy or another right may prevail. When assessing the proportionality of the restriction of a fundamental right, the following steps are usually considered:

---

[97] In the context of this report a security technology is a generic technology or a technology whose purpose of use has not yet been defined. A security product has a defined purpose of use.

- the interference must aim at achieving a legitimate purpose, and
- the interference must be a suitable, necessary and adequate measure to achieve the legitimate purpose.

When restricting a fundamental right the authority authorised to do so is at the same time obliged to apply the least intrusive means that ensures effectiveness. In this context, a product which complies with privacy principles or which is even privacy enhancing will make a proportionate restriction of privacy more likely because it can help to lessen the intensity of the interference with the fundamental right[98].

Following this analysis, governments or public authorities in the role of customers and thus drivers of security technology should, bearing their legal obligations in mind, ask only for security technologies that allow privacy compliant use. Whether compliance with all privacy principles is required when the product is in actual use, is a secondary question.

Furthermore, in the context of FP7 research and funding, a requirement that consortia submitting proposals must consider the privacy impact of their work and must achieve, consider and protect the fundamental rights of European citizens is laid down by the European Commission's distinct postulation.

3.7.4 Conclusion

The security product must generally allow privacy compliant data processing, whether it is going to be used by public authorities or private companies. Restrictions of privacy principles are possible for use by public authorities. However, the specific design of this restriction may vary depending on national law as well as on different ways of use. In order to allow the broad targeting of possible purchasers and in order to allow proportionate use, the security technology must be designed in a way that allows privacy compliant use. A process to operationalise the designing of privacy into technology is described in the following subchapter 3.7.

3.8 Approach to a management process leading to privacy compliant security technologies

In addition to technical means, organisational means are also necessary to ensure the research and development process results in a privacy compliant product. A management process must be implemented in the entity carrying out research and development to provide guidelines as to how and when to consider privacy compliance, privacy impact and mitigating tools. Following the model process, this process should be designed according the cycle stages "plan – do – check – act".

As a first step the research entity has to initialise the Data Protection Management Process by creating a policy regarding firstly what data protection objectives must be met when carrying out research (for example with regard to pilot tests involving natural persons) and secondly which objectives must be observed regarding the final product or technology. ("Plan").

---

[98] See D3.2, page 40.

Personal data must then be processed in accordance with this policy and research must be carried out in accordance with these objectives. (“Do”).

It is essential to monitor observance of these objectives throughout the entire research process. If requirements are not met, prompt countermeasures can be implemented at an early stage. Checks should involve self-evaluation by the researchers assigned to develop the technology (and the immediate reporting of deviations) as well as an evaluation by the relevant work package leader or project manager. To enable these checks, indicators for compliance should be laid down. (“Check”).

Furthermore, deviations and weaknesses identified during this evaluation process must be addressed, and suggestions for amending the policy must be discussed and implemented. (“Act”).

A generic approach to such a process covers the following steps:

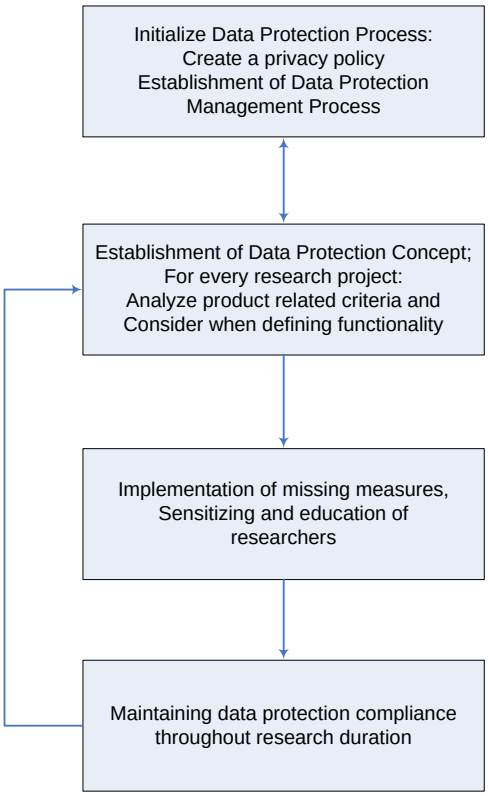

Figure 8: Generic model of a data protection management process for security technology researchers

In addition to this generic approach, a support process should be implemented. In order to maintain data protection compliance throughout the entire duration of the research it is necessary to monitor developments in legislation. If changes in data protection law occur, the policy must be adjusted accordingly.

In addition developments in research on privacy enhancing technologies must also be monitored in order to achieve the design of the least intrusive security technology possible. It can still be possible to consider any new solutions introduced during the project's lifetime. However, if a project has reached an advanced stage, implementing new solutions can face resource restrictions. This should be discussed in the project's Privacy or Ethical Report, which PRISE suggests should be introduced as compulsory for all research projects dealing with security technologies.

Finally, changes and developments in applicable standards or best practice approaches dealing with data protection compliance, the management thereof and established standards in IT Security should also be monitored in order to apply changes to the project's Data Protection Management Process.

Such a generic supporting process to a Data Protection Management Process looks like this:

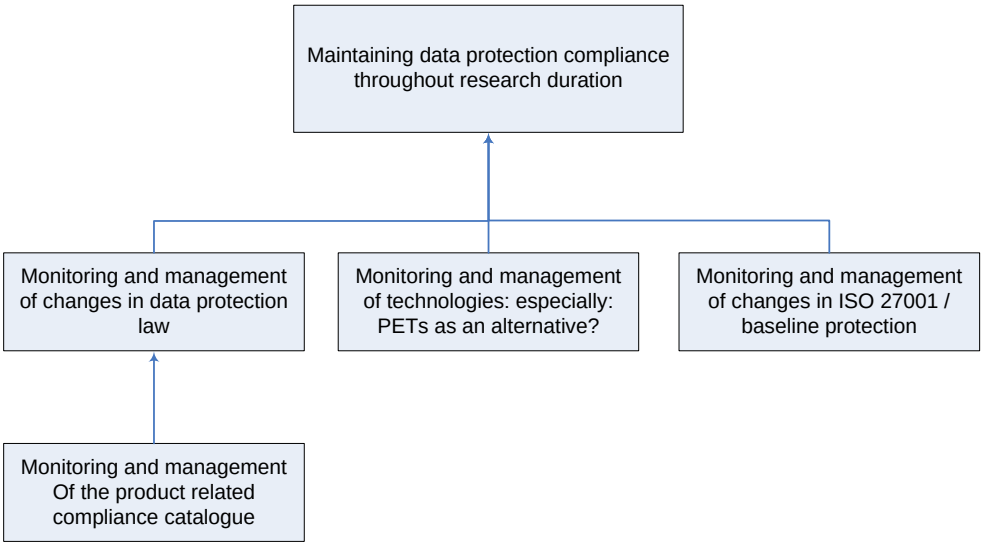

Figure 9: Generic supporting process for Data Protection Management Process

3.9 A generic product related approach: Criteria for privacy compliant security technologies

This subsection focuses on the development of criteria for privacy compliant security technologies which can be used to assess the privacy implications of research projects applying for FP7 funding, and which can be used by developers of security technologies when aiming at a compliant prototype or research result.

In order to identify the implications for general privacy principles, both the research entity and the proposal evaluator can assure that they have covered all possible aspects when conducting a risk assessment. A standardised approach to identifying risks to general privacy principles

involves a comprehensive set of questions pointing to existing risks. The check lists for evaluators and proposal writers presented later (see 4.3) are condensed versions of the sets of questions for each privacy principle presented here.

D3.2 The Legal Report extracted the following general privacy principles which must be observed:

- Legitimacy
- Purpose binding
- Proportionality
- Transparency
- Quality of data
- Security of data

A generic approach, taking into account the aforementioned information security standards and approaches would look like this:

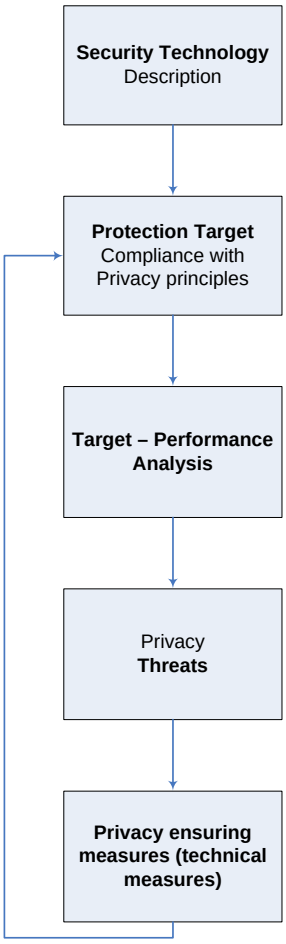

Figure 10: Generic product-related approach for criteria

The application of this generic approach should be supported by the following set of questions:

I. General Issues	**Observation: yes / no / further explanation**
What type of personal data will the security technology process?	
Does the technology process (allow for the processing of) sensitive personal data?	
Does the technology process (allow for the processing of) intimate personal data?	
Does the technology differentiate sensitive or intimate data from other forms of personal data and are these types of data processed in a different way?	
What is the purpose for which the technology will be used and personal data processed?	
Can the technology be used for further purposes (function creep) and if so, which purposes?	
Does the technology allow transmission to third parties or disclosure (within the data controlling entity or externally)?	

II. Legitimacy	**Observation: yes / no / further explanation**
Is the use of this specific technology and the data processing enabled by this technology covered by a legal provision?	
If sensitive data is to be processed, how is the data subject's unambiguous consent ensured?	
Is a national identification number or another unique identifier processed? For what reason and based on which legal provision?	
Does the technology enable the processing of traffic data or location data? Is processing covered by a legal	

II. Legitimacy	**Observation: yes / no / further explanation**
provision?	
Are the sources of the data recorded (especially if data fusion / sharing is intended)?	
Is data collected or stored secretly / unobserved or are individuals made aware that their personal data is being processed?	
Does the technology allow only for use / access by authorised personnel? How? Is any access and use logged?	
Does the technology contain an interface or is it intended to share data with any third party? Is any such disclosure to third parties logged?	
Does the technology merge, use and/or mine data from other sources? Is this use of data logged?	
If data is disclosed to third parties, is only data passed on that is needed for the distinct purpose?	
Is data automatically anonymised or pseudonymised upon disclosure to a third party?	

III. Purpose Binding	**Observation: yes / no / further explanation**
Is the purpose for which the data was collected recorded and “linked” with the data?	
Does the technology allow the allocation of different access rights for different sets of data which were collected for different purposes?	
Does the technology ensure data is only used for the purpose it was collected for?	
Is the processing logged in order to enable identification of misuse?	

III. Purpose Binding	**Observation: yes / no / further explanation**
Does the technology enable processing of data for a purpose other than the original one?	
What checks are implemented to ensure that further processing is not incompatible with the original purpose?	

IV. Proportionality	**Observation: yes / no / further explanation**
Does the technology support an assessment of the adequacy of personal data for each purpose determined?	
Does the technology collect and process no more data than the minimum required for the purpose for which it is collected?	
Is it possible to set and later change automated retention periods / data deletion?	
Is data reviewed as to whether it is still necessary for the purpose for which it was collected?	
Does use of the technology affect an undefined number of individuals?	

V. Transparency	**Observation: yes / no / further explanation**
Is data collected or stored secretly / unobserved or are individuals made aware that their personal data is being processed?	
Does the technology allow logging of data collection and processing in order to allow later notification and judicial scrutiny?	
Does the technology involve the taking of fully-automated decisions and does it allow for (later) notification of the data subject?	

V. Transparency	**Observation: yes / no / further explanation**
Does the technology use data from third parties and is this data marked?	

VI. Quality of Data	**Observation: yes / no / further explanation**
Does the technology allow for rectification of incorrect data?	
Does the technology enable the accuracy of personal data to be checked with the data subject concerned?	
Are the sources of personal data recorded and is rectification of data reported to these sources?	
How long is data stored?	
Is there an automated initiation of an accuracy check or an updating process in place?	
Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?	

VII. Security of Data	**Observation: yes / no / further explanation**
Does the technology prevent unauthorised access and use?	
If sensitive data is processed, are there safeguards for higher protection of this type of data in place?	
Are procedures in place to detect breaches of security?	
Is encryption used to protect personal data? How are keys handled?	
How is unauthorised copying of personal data prevented?	

VII. Security of Data	**Observation: yes / no / further explanation**
Does the technology comprise mechanisms to prevent accidental loss of data?	
Does the technology allow for the destruction of data no longer needed?	
Are third parties involved in data processing?	

Where the application of these sets of questions indicates open issues and risks to privacy, the consortium must discuss solutions and mitigating tools in its proposal. Many of the available approaches for privacy enhancing technologies are described in D3.3 Proposal Report. Further technical and organisational measures are presented below (4.3).

3.10 A process- and organisations-related approach to the privacy-aware use of security technologies

Finally, it should be considered that even if a security product allows privacy compliant use, a severe and yet unnecessary impact on privacy can result from negligent or incorrect use. Consequently, an organisation related process of data protection management within the organisation completes the PRISE approach towards privacy compliant security technologies (use): presented here

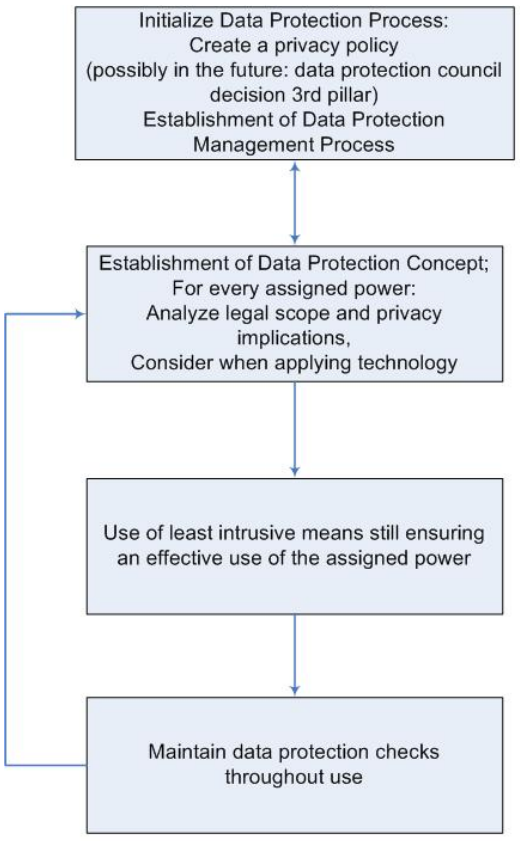

Figure 11: Generic organisation related process for the user of security technology

Personnel should be given training in privacy, data security and risk management to enable them to become aware of the existing privacy policy.

In addition to this generic approach a supporting process should be implemented to ensure that the least intrusive means are identified and proportionate technology use is carried out:

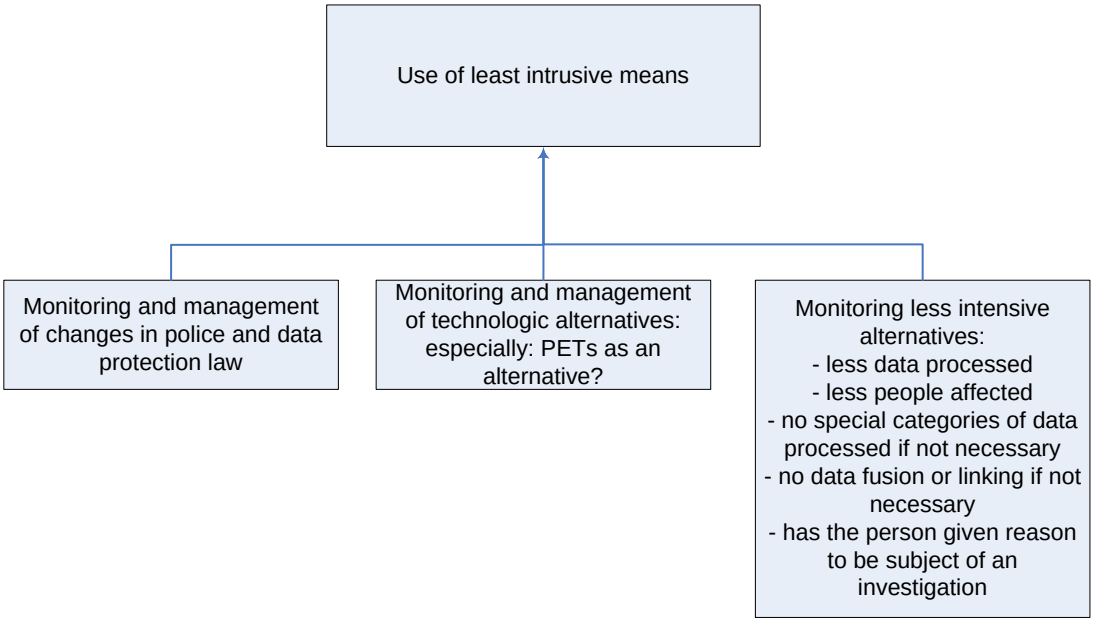

Figure 12: Generic approach to the supporting process of user data protection management process

3.11 Summary

With regard to information security management and privacy or data protection management a number of methods, organisational structures and management systems are established. They cover important phases of the life cycle of products and business or governmental procedures. A number of certificates are already available to certify compliance with good practice information security management models and privacy or data protection legislation. While some information security certificates are standardised at an international level, (ISO standards and CC), privacy seals and data protection audit schemes can be applied on a national or even regional level only. The reason is the differences in data protection legislation that exist worldwide and even within Europe, because the European Data Protection Directive 95/46/EC has been implemented differently in different national legislation. However, with the start of the EuroPriSe project, this may well change in the future.

The following table lists existing approaches in information security management and privacy or data protection management in comparison:

Area of Application	Information Security	Privacy and Data Protection
Development of technologies (purpose of use not defined yet)	Technology Impact Assessment / **Attack Tree Analysis**	Technology Impact Assessment / **Privacy Impact Assessment (PIA)**
Products (purpose of use defined)	**Common Criteria, ISO 15408** (contain among others: security targets, corresponding security functions, strength of function and evaluation assurance level) **Methods: CC methodology in combination with supporting methods e.g. Attack Tree Analysis**	**Privacy Seals** (certify that privacy protecting design and / or Privacy Enhancing Technologies (PETs) are used in the product and the product can be used in a manner that is compliant with data protection legislation) **Method: Compliance analysis at a legal and technical level with privacy or data protection legislation**
Business and governmental procedures (purpose of use well defined)	**ISMS, ISO 27001 and following standards such as BSI baseline protection** **Methods: Risk Assessment and supporting methods** such as FIA and Attack Tree Analysis **Good practice for process models and organisational structures** (e.g. information security officers, information security management team etc.)	**National and regional Audit Schemes** **Method: Compliance analysis at a legal, organisational and technical level with privacy or data protection legislation** **Good practice for organisational structures** (e.g. privacy commissioners, data protection advisors)
Public and private organisations (Policies for information security and privacy are available)	**ISMS, ISO 27001 and following standards such as BSI baseline protection** **Methods: Risk assessment and supporting methods** such as FIA and Attack Tree Analysis **Good practice for process models and organisational structures** (e.g. information security officers, information security management team etc.)	**Private, national and regional audit schemes** **Method: Compliance analysis at a legal, organisational and technical level with privacy or data protection legislation** **Good practice for process models and organisational structures** (e.g. privacy commissioners, data protection advisors)

Table 4: Comparison of information security and privacy protection management

4 The PRISE Criteria Matrix in practice

The PRISE matrix presents a systematic approach for the analysis of the privacy impact of a technology under development and its subsequent use.

Privacy compliance is not only a matter of the technical design of the future technology. In the end the legal basis regulating and permitting technology use as well as the specific use of the technology by the end user (e.g. law enforcement authorities) also impact the privacy relevance of putting security technologies to use. For consortia intending to develop a new security technology, this means they not only have to focus on the technical features of their subject of research. It is also essential to design the technology in a way that allows subsequent use to be legally compliant with the applicable national legislation. If a technology is to be used in several member states or third countries, the initial design may even need adjustment to meet different national requirements. Generally speaking, in order to increase the likeliness of proportionate use, the technology should be designed by making use of PET design options[99]. Furthermore the technology should contain features that support the Data Protection Management Process approach presented above. This includes in particular measures that support organisational tools like supervision in the user entity, tools enabling later or immediate transparency for the data subject, as well as tools ensuring that only authorised use of the technology is possible (which again has to be supervised). This combination of technical features supporting organisational measures will increase usability for security technology users, help them to comply with their legal obligations and, if designed in the right way, fit into the organisational processes existing in the entity using it.

The matrix is arranged in three stages[100], each of which should be considered by the consortium applying for funding as well as the evaluator assessing the proposal. The proposal must indicate what kind of data is going to be collected and processed with the new security technology. If it allows for the collection of intimate data, the technology will face significant problems in Germany[101]. In other member states, proportionate use of a technology allowing the collection of intimate data is difficult for the users to conduct. If the technology also allows for the collection and processing of intimate data, the proposal should discuss which safeguards are implemented to assure that this kind of data is not collected and processed. As a second step the proposal writer should discuss how and whether the general concept of the new technology as well as specific features might infringe the privacy principles described in D3.2 Legal Report. The PRISE matrix remains rather abstract on the 'question level' of stage 2 (data protection compliance) in order for the matrix to remain usable. Several detailed and helpful tools exist to assess the privacy impact and privacy compliance of projects and products.[102]

---

[99] See also D3.3 Proposal Report.

[100] See Chapter 3 – the PRISE approach.

[101] The German constitutional court ruled there has to remain a so called core sphere (*Kernbereich*) or place of last retreat free from covert surveillance. The collection and processing of intimate data always affects the fundamental right of human dignity. In German constitutional law an infringement of human dignity allows for no weighing of the infringed right against the rights protected. An infringement of Article 1 Basic Law which protects the fundamental right of human dignity is always unlawful and there is no room for an assessment of proportionality here under German law. BVerfGE 109, 279; 113, 348.

[102] To name only three, proposal writers can refer to the EuroPriSe project's handbook to assess compliance with European Data protection law and the ICO's PIA Handbook which focuses on impact on general privacy principles. Furthermore, also the CEN's Personal Data Protection Audit Framework (CWA 15599-1 and -2) can be consulted.

Finally, the proposal needs to address the social impact and aspects of the research applying for funding. New refined and more efficient security technologies may introduce new technical features, which can reduce or increase the technology's impact on privacy as well as on security. Since there are security solutions for the investigational powers of many law enforcement authorities the proposal will have to indicate not only how it differs from existing security technologies. It must also discuss how the security technology aims to foster security[103] and how the expected security gain relates to the identified privacy risk. Since the matrix will point the FP7 evaluator to open issues, a lack of discussion in the proposal may have negative consequences for the evaluation of the proposal.

For each of the three levels, proposal writers and evaluators can turn to the PRISE handbook (Chapter 4.3) for available tools that address the identified privacy issues.

In order to allow a systematic overview of privacy issues, PRISE suggests the application of two Privacy Check tables, one for evaluators and one for proposal writers. These tables provide for a more detailed assessment of a proposal's privacy impact than the ethics table currently used in FP7 proposal templates. It refers to the PRISE matrix's three levels. Filling in the table will be self-explanatory for proposal writers after having applied the PRISE matrix and the description presented in this report to the intended subject of research.

The proposal evaluator will be able to systematically assess whether the proposal affects privacy issues of the intended research and discusses tools to mitigate or reduce privacy implications. The Evaluator's privacy check table suggests assigning red or green lights depending on whether a tool was identified to address the privacy issues found.

It is not for the PRISE project to present recommendations regarding how many red lights ought to lead to a proposal being rejected, as this decision must be based on the overall impression of the proposal. An assessment will take into account the characteristics of each proposal and a standardised balancing of the results seems inappropriate. The aim of the PRISE approach is to enable proposal writers and proposal evaluators to take a systematic approach regarding privacy implications. The PRISE approach is intended to support a comprehensive analysis and ensure that both parties involved in the application process consider all relevant aspects.

[103] Security of the individual or the state? See Chapter 2 for description of different concepts of 'security'.

4.1 Privacy Check for proposal writers

	YES	HOW? ➔see Proposal page
Relevance of the issue		
Does the proposed technology involve processing personal data (e.g. data that makes people identifiable)		
Does the proposed technology involve tracking the location or observation of people?		
Core Sphere		
Does the proposed technology interfere with human dignity?		
Does the proposed technology interfere with the physical integrity of people?		
Does the proposed technology allow or aim at interaction with partners like spouses, children, lawyers, priests?		
Data Protection Compliance		
Does the technology lack a specification of the purpose of use and data collection or is the purpose stated very broadly?		
Does possible technology use and data collection and processing require the adoption of a new legal basis?		
Is there a less intrusive means available to allow the achievement of the intended result with comparable efficiency?		
Does the technology aim at or allow the collection of sensitive data? (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical persuasion)		
Does the technology involve the linking of data, data fusion or data analysis?		
Does the technology require lifting the anonymity of data subjects?		
Is the technology used regardless of whether the individual is suspected of any wrongdoing?		
Is lack of transparency regarding technology use (prior to and/or after use) the default setting?		
Context sensitive trade-off		
Does the proposed technology enhance privacy compared to existing solutions?		
Does the proposed technology aggravate judicial scrutiny?		
Does the proposed technology facilitate human societal security?		
Is the proposed technology aimed at crime prevention?		
Is the proposed technology aimed at prosecution?		
Is the main field of application the struggle against… terrorism organised crime random crime		
Does the proposed technology increase individual security against the state (in terms of privacy protection) other spheres (economy, social)		

Table 5: Privacy Check for proposal writers

4.2 Privacy Check for Evaluators

	Tools	Red/green light
Relevance of the issue		
Does the proposed technology involve processing personal data (e.g. data that makes people identifiable)		
Does the proposed technology involve tracking the location or observation of people?		
Core Sphere		
Does the proposed technology interfere with human dignity?		
Does the proposed technology interfere with the physical integrity of people?		
Does the proposed technology allow or aim at interaction with partners like spouses, children, lawyers, priests?		
Data Protection Compliance		
Does the technology lack a specification of the purpose of use and data collection or is the purpose stated very broadly?		
Does possible technology use and data collection and processing require the adoption of a new legal basis?		
Is there a less intrusive means available to allow the achievement of the intended result with comparable efficiency?		
Does the technology aim at or allow the collection of sensitive data? (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical persuasion)		
Does the technology involve the linking of data, data fusion or data analysis?		
Does the technology require lifting the anonymity of data subjects?		
Is the technology used regardless of whether the individual is suspected of any wrongdoing?		
Is lack of transparency regarding technology use (prior to and/or after use) the default setting?		
Context sensitive trade-off		
Does the proposed technology enhance privacy compared to existing solutions?		
Does the proposed technology aggravate judicial scrutiny?		
Does the proposed technology facilitate human societal security?		
Is the proposed technology aimed at crime prevention?		
Is the proposed technology aimed at prosecution?		
Is the main field of application the struggle against…		
terrorism		
organised crime		
random crime		
Does the proposed technology increase individual security against		
the state (in terms of privacy protection)		
other spheres (economy, social)		

Table 6: Privacy Check for Evaluators

4.3 The PRISE-Handbook

This handbook lists identified tools addressing privacy issues of security technologies. Many of them have already been presented in D3.3 Proposal Report. For these, a reference will be provided in order to avoid reiteration. Tools cannot be presented for all privacy issues, especially not the technical tools which are the obvious focus of security technology R&D. Security technologies can be designed to be privacy friendly but they will usually still infringe privacy in the end. Existing laws may well cover this infringement. As indicated in D3.3 Proposal Report, a restriction of privacy to safeguard national security, public security or e.g. the prevention, investigation, detection and prosecution of criminal offences are generally permissible under Art. 13 of Directive 1995/46/EC. With technologies which are not available for use by private entities, the restriction of privacy rights and principles can thus be lawful.

As explained in D3.2, compliance with the principle of proportionality as well as the principle of legitimacy is however always mandatory. And it is in this context that technologies that also comply with other privacy principles will increase legal certainty for the technology user that he or she is conducting a proportionate use. In particular, restrictions of the right of transparency at the moment of technology use can and should be met by technology features allowing later scrutiny by a court of law, supervision of technology use by the management or head of the using entity, and notification of and access to the collected data by the data subject. This means that even though the technology may for example already by virtue of its purpose (covert surveillance) not provide immediate transparency, it has to enable and assist the user to comply with other legal obligations which are usually in place for all investigational measures. A discussion of how the technology, if it restricts privacy on the one hand, fosters data subjects' rights on the other is advisable as a means to show that research is focussing on developing security technologies acceptable to European citizens.

The following description of tools maps the three steps presented in the PRISE matrix as well as the questions presented therein that lead to the identification of privacy issues.

4.3.1 Minimum level of privacy

The minimum level of privacy protection as a baseline is applied to human dignity, physical integrity and intimate data. The term 'intimate data' is not equivalent to special categories of data as laid down in Article 8 of Directive 1995/46/EC. For this kind of data, the processing of which affects human dignity, collection and processing is not permissible in Germany, and risks not being proportionate in other member states: In addition to the ethical implication of processing intimate data in the course of an investigation, the effectiveness and thus necessity of processing intimate data is doubtful. If an investigation turns on allegations of sexual assault , the views held by the suspect are also of relevance. Otherwise, a citizen's inner thoughts and views as well as intimate acts must remain the citizen's last place of retreat from state surveillance. It does not matter whether these thoughts are expressed in a very private conversation or written down in a diary.

Surveillance technologies will often allow for the collection of intimate data. This is the case e.g. for optical and acoustic surveillance such as video surveillance, wiretapping and

eavesdropping. Furthermore, the investigative power to conduct an 'online search[104]' of a suspect's computer as currently being discussed may involve the collection and processing of intimate data.

The citizens' involvement in Work Package 5 revealed serious concerns regarding technologies that invade the bodily private sphere such as scanning machines like the 'naked machine'. This view indicates that an intrusion into a person's private sphere, which is at the same time perceived to violate human dignity, is not acceptable to citizens.

Technologies which allow for the collection and processing of intimate data face one problem: it is currently not possible for a technology to automatically analyse data collected as to whether it is intimate data. For written data an assessment of what kind of data is contained in a text file must involve an analysis and thus access to the data. While for the collection of optical and acoustic data it is possible to have a law enforcement officer monitor the collection live and to interrupt the data collection immediately it becomes evident that the collection now comprises intimate data, this is not possible for the covert online search of a computer and the processing of data stored on it.

The requirements listed here are not tools in the sense that they could justify the processing of intimate data. However, since the processing of intimate data should be avoided in order to increase the possibility of a proportionate policing measure, technology design should comprise the following requirements.

Technological requirements

Security technologies which allow covert surveillance must consequently allow for **live monitoring** of the data collection, an **interruption** of the collection and the **deletion** of wrongfully collected data. If live monitoring is not possible and hence collection of intimate data cannot be prevented immediately, the technology most likely does not comply with at least German legal requirements. Furthermore, to allow an assessment of whether intimate data was not first collected, analysed or used and then deleted, the technology must include **logging** of who is using the technology, the time and duration of use, actions initiated by the user and the point of time when they were initiated. Examples of technical tools to prevent interference with human dignity or physical integrity could be e.g. an integrated feature of scanning devices to automatically suppress body parts and only show the suspect material. Another feature could be the creation of automatic erasing processes and expiry dates for data. Furthermore it seems necessary that technologies at stake allow the implementation of legal restrictions on use and subsequent checks on the legality of use. This includes revocability and limitation of functionality (in addition to the tools above).

---

[104] An online search involves as a first step the infiltration of the suspect's computer. This can be achieved by gaining physical access to the computer and installing a backdoor software ('trojan horse'), by sending an email attachment containing a backdoor software to the suspect together with an incentive to open the attachment, or by gaining online access to the suspect's computer for example by means of exploiting operating system security flaws and installing a backdoor software. As a second step the installed backdoor allows the law enforcement officer to gain access to the suspect's computer and can e.g. be used to transmit data stored on the suspect's computer to the law enforcement authority. Furthermore, the software installed to infiltrate the system can also contain a keylogger used to record the suspect's passwords used for example for encryption of files. For a description of the possible technical background of online search see Hansen, M. and Pfitzmann, A.: 'Technische Grundlagen von Online-Durchsuchungen und -Beschlagnahme', 2007. Available online at https://tepin.aiki.de/blog/uploads/hansen-pfitzmann-online-durchsuchung-und-beschlagnahme-1.0.pdf.

Organisational safeguards

If such a logging should for some reason – which would require comprehensive explanation in the proposal – be impossible to implement, a fallback option is an organisational tool. In order to make the technology user aware of the sensitive nature of the data that can be collected, the technology developer must provide the user with **written information** on this topic as well as a **draft form for manual logging** of the aforementioned points by the law enforcement officers using the technology.

Concerning technologies interfering with human dignity or infringing the integrity of the body it may be possible to circumvent problematic monitoring situations by physically dislocating staffers and the persons scanned, so that they cannot be seen "personally".

In addition, on the side of the using entity, **internal training** for personnel concerned with investigations and use of security technologies is advisable. Users of security technologies must be aware of impacts on fundamental rights that their daily duties during investigations involve. Personnel using security technology should be trained with regard to the sensitivity of different kinds of data (intimate data, special categories of data, other personal data). Emphasis should be put on considerations of data avoidance, if processing of intimate data has no relevance and effectiveness for the allegations under investigation. Furthermore, the entity using security technology should draw up a **monitoring process** of lawful technology use as part of a **data protection management process** (see 3.8).

Legal tools

Germany has imposed a legal prohibition on even the collection of intimate data, since collection already means an infringement of human dignity. All laws adopted must comply with this requirement.

In other member states the type of data collected can impact on the proportionality of the measure.

Special legal tools justifying processing of intimate data do not exist.

For new security technology applications, it may be necessary to create new rules that prohibit the showing, storing and processing of data that infringes human dignity or the physical integrity of persons. Other legal tools may be the establishment of new control institutions, the duty to involve DPAs, NGOs or privacy consultants in the technical design process.

4.3.2 Data protection and privacy compliance

A focus of PRISE is on criteria for data protection and privacy compliance. In order to be able to assess compliance of planned research and a technology under development, a consortium should take a systematic approach to understanding the privacy impact of their work. Only if a precise analysis of the kind of personal data processed, data flows, access rights to stored data, data transmission to third parties, analysis and use of stored data etc. is carried out, will the consortium then be in a position to identify possible privacy risks as well as mitigating tools. Questions supporting this analysis are presented in 3.7.

Technical tools

Technical tools to foster and enforce compliance with privacy laws are known as PETs. An introduction to and presentation of PETs is given in D3.3 Proposal Report. The following goals are to be pursued in enhancing the data subject's privacy:

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

An in-depth description of these goals is presented in D3.3. Identified tools broken down according to the privacy principles applied in PRISE cover:

Privacy Principle (as identified in D3.2)	PETs as a technical tool
Legitimacy	Control of the user, sticky policies
Purpose Binding	Unlinkabililty, control of the user, pseudonymity, sticky policies
Proportionality	Data minimisation, anonymisation
Transparency	Transparency
Quality of data	Data subject's rights to access, rectify data
Security of data	Security of data, sticky data tracks

Table 7: Privacy principles and related PETs

In order to ensure the auditability of processing, the **logging** of access to personal data and of data processing is necessary. As log files usually contain personal data of the data subject and of the individual processing the data, these files are also subject to data protection regulations. The processing of log files thus has to be secured by technical and organisational measures, too.

Network and transport security as objectives of IT infrastructure security and the security of transmitted data must be ensured.

Organisational tools

A main duty for data controllers is the **prevention of unauthorised access** to data, programs, premises and devices. Where applicable, physical access control and access control to mobile devices must be implemented. Identification and authentication must be ensured. Typical mechanisms comprise login names and passwords, biometrics, security tokens, and cryptographic keys. The management of access control must be carried out as part of the Data Protection Management process.

An approach for a management process leading to privacy compliant security technology **research** is presented at technology research is presented in Chapter 3.6.

A process and organisations-related approach to the privacy aware **use** of security technologies is elaborated in Chapter 3.8.

Legal tools

This report has discussed the term security and different perspectives of security. An assessment of a law's expected security gain is difficult to conduct as it requires an ex ante forecast of expected threats and a technology's ability and probability to reduce these threats. However, assessing a law's privacy impact is easier since the scope of this fundamental right as well as its infringement is caused by the technology use itself. It is necessary to conduct a privacy impact assessment of a draft law prior to its adoption. Complying with the proportionality principle is mandatory not only for security technologies but also for the legal basis allowing their use.

As passing security laws involves an ex ante assessment of the expected security gain and privacy impact, it is consistent to evaluate whether the forecast prognosis came true. Laws introducing new or extending existing law enforcement powers have an impact on privacy and data protection. After a short period new laws should be evaluated and sunset clauses should be introduced into new security laws: if no evaluation is conducted or the evaluation finds that the security gain facilitated by the law is small in comparison to a significant privacy infringement, the law should be amended.

In order to emphasise a minimum level of privacy protection, member states should consider regulating a minimum level of privacy. Additionally there should be an institutionalised approach to monitoring the necessity for specific regulations for (emerging) technologies with intense impact on privacy.

The scope of Directive 1995/46/EC should be extended and its obligations should be addressed by the developers of security technologies and all technologies which are used for any stage of data processing.

A legal obligation should be introduced for entities using security technologies to implement a (certified) data protection management process.

Public authorities should be obliged to use only privacy certified security technologies.

And finally, preventive investigations without a concrete suspicion of a criminal act should be a last option and require a concrete enumeration of the serious crimes that may initiate the investigative measure.

4.3.3 Context sensitive trade-off

The third level of the PRISE-Matrix deals with context sensitive trade-offs i.e. situations in which security technologies may be applied in a manner that is not data protection compliant. These situations call for a high awareness of the severe concern at the intrusion into individuals' privacy. It is possible and sometimes necessary to do so. It is all about weighing and proportionality. This means it is necessary to look at the two sides of an equation: on the one side is the security of individuals, institutions and societies and on the other is the

infringement of fundamental rights of individuals. The tools presented above aim at ensuring that security technologies infringe privacy to the least possible extent. In specific situations it is necessary to apply security technologies in a manner that is not privacy compliant. If so, there should be procedures that highlight the security gain for individuals or societies that emerges from the privacy-incompliant way of using security technologies.

Technical tools

Technological means used in this respect are so-called PETs. Privacy enhancing technologies may be a way of saving individuals' privacy and preventing misuse of the gathered data while keeping the technologies effective.

Proposers and evaluators should always consider technical or organisational alternatives too. If there is another, less intrusive means, it would produce a red light for a privacy intrusive technology system.

The aim of developers of security technologies should be to minimise the PID needed to fulfil the task. If it can be shown that the same or even a better effect could be gained with new technology by processing less PID than in previous versions, the technology would be rated better.

Anyway, there should be attempts to increase security without processing PID. Arguably, it would be best to increase the efficiency of prevention by decreasing the likelihood or effect of potential attacks

Organisational tools

It is not possible to forecast the security gains of the implementation of a specific security technology. It is only possible to argue how the specific technology is supposed to increase the security of society. It is necessary to describe in detail the functions and their supposed impact. To foster the argumentation, it could be helpful to present experiences from other similar technologies (older versions) and or to discuss the advantages and disadvantages of the technology in question and its alternatives. This argumentation must withstand a plausibility check by experts and should be supported by data from the past.

As far as crime prevention and prosecution are concerned, the hypothesis provided is that successful prevention brings a higher security gain than laying the focus on prosecution only. Therefore part of the proposal should be a discussion whether a technology is better used for prevention or prosecution.

In terms of effectiveness, technologies that try to enhance objective security are more suitable than those that just raise the subjective security feeling. This again leads back to a plausible argumentation of all aspects of security gain that the technology in question promises.

The assessment of alternatives, be it organisational procedures or technological alternatives, is supposed to be an integral part of any security gain assessment. Any security technology should be re-evaluated after some time of use.

The possibility of targeting the technology at small groups of people or to suspects only should be reflected in organisational and possible technical features. The presentation of the features of the technology in question should also comprise statements about the main target of the

technology. Can it be used in the fight against terrorism, against organised crime or random crime? The threats coming from these arenas should be estimated.

Legal Tools

With regard to privacy and data protection, proportionality is a core concept and is laid down in several laws[105] around the EU. The main legal instrument used is the necessity of getting a court order before using privacy-infringing technologies. Participants of the six European participatory events specifically highlighted court orders during this PRISE project. It seems to be a well-established tool that ensures independent control and oversight. This makes the citizen feel comfortable and builds trust even in situation when privacy-intruding measures are taken. In order to build trust in and acceptance of security technologies it seems wise for technology developers as well as for further users and politicians to ensure that the instrument retains its high rating.

Principles to follow could be to protect individual security and to avoid the restriction of as many privacy principles as possible to achieve proportionality between privacy loss and security gain.

[105] See also D3.2 Legal Evaluation Report

References

Bennett, C. J. und Raab, C. D., 2003, The Governance of Privacy, Aldershot, Hampshire GB: Ashgate.

Bock, K., EuroPriSe – Das Datenschutz-Gütesiegel aus Schleswig-Holstein wird europäisch, 2007, Datenschutz und Datensicherheit 6/2007, 410.

Bundesamt für Sicherheit in der Informationstechnik, 2005, BSI-Standard 100-2 IT-Grundschutz Methodology Version 1.0. Available at http://www.bsi.de/english/publications/bsi_standards/standard_1002_e.pdf.

Bundesamt für Sicherheit in der Informationstechnik, 2008, BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz Version 2.5,. Available at http://www.bsi.de/literat/bsi_standard/standard_1003.pdf.

Bundesamt für Sicherheit in der Informationstechnik, BSI-Standards. Available at http://www.bsi.de/literat/bsi_standard/index.htm.

Bundesamt für Sicherheit in der Informationstechnik, Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik. Available at http://www.bsi.de/cc/index.htm.

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz Allgemeine Informationen. Available at http://www.bsi.de/gshb/zert/index.htm.

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz. Available at http://www.bsi.de/gshb/index.htm.

Bundesamt für Sicherheit in der Informationstechnik, IT-Sicherheitskriterien und Evaluierung nach ITSEC. Available at http://www.bsi.de/zertifiz/itkrit/itsec.htm.

Bundesamt für Sicherheit in der Informationstechnik, Safeguards Catalogue Infrastructure IT Baseline Protection Manual. Available at http://www.bsi.de/english/gshb/manual/download/safeguard-catalogue.pdf.

Bundesamt für Sicherheit in der Informationstechnik, Threats Catalogue IT Baseline Protection Manual. Available at http://www.bsi.de/english/gshb/manual/download/threat-catalogue.pdf.

BVerfG, 1 BvR 518/02 vom 4.4.2006, Absatz-Nr. (1 - 184), Available at http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html.

BVerfGE, Volkszählungsurteil, 65(1), 42f.

Clarke, R., Privacy Impact Assessment, 2003. Available at http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html#App.

Conference on Security and Co-operation in Europe (CSCE) 1975, Helsinki Final Act, Available at http://www.osce.org/item/4046.html.

Daase et al. 2002, Internationale Risikopolitik – der Umgang mit neuen Gefahren in den internationalen Beziehungen, Baden-Baden

Department of Homeland Security's Privacy Office, Privacy Impact Assessment. Available at http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.

Di Fabio, U., 2008, Sicherheit in Freiheit, Neue Juristische Wochenzeitschrift 2008 (No. 7).

Egger, E., 1990, Datenschutz versus Informationsfreiheit – Verwaltungstechnische und verwaltungspolitische Implikationen neuer Informationstechnologien; in Reihe: Schriftenreihe der Österreichischen Computer Gesellschaft, Bd. 52, hg. v. OCG, Oldenbourg, Wien, München: Oldenbourg.

Elias, N., 1978, Über den Prozeß der Zivilisation. Soziogenetische und psychogenetische Untersuchungen. Bd I: Wandlungen des Verhaltens in den weltlichen Oberschichten des Abendlandes; Bd. II: Wandlungen der Gesellschaft. Entwurf einer Theorie der Zivilisation.: Suhrkamp Taschenbuch.

Endruweit, G., 1989, Wandel, sozialer, in: Endruweit, G. und Trommsdorf, G. (Hg.): Wörterbuch der Soziologie, Stuttgart: Enke, 798-805.

Erikson, J. and Giacomello, G., (Eds.), 2007, International Relations and Security in the Digital Age, London/NewYork

ESRAB, 2006, "Meeting the Challenge", Available at http://ec.europa.eu/enterprise/security/articles/article_06_09_25_tc_en.htm.

European Commission, 2003, A Secure Europe in a Better World – European Security Strategy (ESS – 12/2003), Available at http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/reports/78367.pdf.

European Committee for Standardization, 2006, CEN Workshop Agreement 15499-1 Personal Data Protection Audit Framework Part I: Baseline Framework – The Protection of Personal Data in the EU, Available at http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cen+workshop+agreements/dppcwa.asp.

European Committee for Standardization, 2006, CEN Workshop Agreement 15499-2 Personal Data Protection Audit Framework Part II: Checklists, questionnaires and templates for users of the framework. Available at http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cen+workshop+agreements/dppcwa.asp.

European Parliament, 2007, Resolution of 12 December 2007 on the fight against terrorism, Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0612+0+DOC+XML+V0//EN Site visited 15th December 2007

Flaherty, D., , 2000, Privacy Impact Assessments: an essential tool for data protection. Available at http://www.anu.edu.au/people/Roger.Clarke/DV/PIAsFlaherty.html.

Foucault, M., 1994, Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt/Main: Suhrkamp.

Geschonneck, A., 2006, Computer-Forensik: Computerstraftaten erkennen, ermitteln und aufklären.

Gridl, R., 1999, Datenschutz in globalen Telekommunikationssystemen; in Reihe: Frankfurter Studien zum Datenschutz, Bd. 12, hg. v. Simitis, S., Baden-Baden: Nomos Verlagsgesellschaft.

Group of Personalities Report, 2004, Research for a Secure Europe, March, Available at http://europa.eu.int/comm/enterprise/security/doc/gop_en.pdf.

Hafskjold, C., 2007, PRISE - Privacy enhancing shaping of security research and technology, Deliverable 2.2 Overview of Security Technologies, Revision 1, Available at http://prise.oeaw.ac.at/docs/PPRISE_D2.2_Overview_of_Security_Technologies-Revision1.pdf.

Hanemann, A., Schmitz, D. and Sailer, S., 2005, A Framework for Failure Impact Analysis and Recovery with Respect to Service Level Agreements. Available at http://www.mnm-team.org/pub/Publikationen/hss05c/PDF-Version/hss05c.pdf.

Hansen, M. and Pfitzmann, 2007, A.: 'Technische Grundlagen von Online-Durchsuchungen und -Beschlagnahme'. Available at https://tepin.aiki.de/blog/uploads/hansen-pfitzmann-online-durchsuchung-und-beschlagnahme-1.0.pdf.

Hayes, B., 2006, Arming Big Brother – The EU's Security Research Programme, Transnational Institute, TNI Briefing series 2006/1

Information Commissioner of the UK, PIA Handbook. Available at http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html.

Jacobi, A. and Holst, M., 2008, PRISE - Privacy enhancing shaping of security research and technology, Deliverable 5.8 Synthesis Report. Available at http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf.

Jacobi, A., 2007, PRISE - Privacy enhancing shaping of security research and technology, Deliverable 5.1 Questionnaire and interview guidelines. Available at http://www.prise.oeaw.ac.at/docs/PRISE_D5.1_Questionnaire_and_Interview_Guidelines.pdf.

Landesbeauftragter für Datenschutz und Informationsfreiheit Bremen, Auditierung von DV-Verfahren und Gütesiegel nach dem Bremischen Datenschutzgesetz. Available at http://www.datenschutz-bremen.de/audit.php.

Lyon, D. (Hg.), 2003, Surveillance as Social Sorting. Privacy, Risk and Automated Discrimination, London: Routledge.

Lyon, D., 2007, Surveillance Studies – An Overview: Polity Press.

Mack, Andrew, forthcoming, 'Data Issues' cit. in Owen 2004.

Meints, M., 2007, Datenschutz durch Prozesse, Datenschutz und Datensicherheit 2/2007, pp. 91-95.

Möchel, E., 2008, Ein Monster aus dem Hause Siemens; Futurezone, Available at http://futurezone.orf.at/it/stories/267116/.

ÖAW, 2005, Sicherheitsforschung, Begriffsfassung und Vorgangsweise für Österreich, Vienna.

Office of Government Commerce, ITIL the key to managing IT services. Available at http://www.ogc.gov.uk/guidance_itil.asp.

Organisation for economic co-operation and development (OECD), EOCD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

Owen, T., 2004, Defining and measuring human security, Human Rights, Human Security and Disarmament, disarmanet forum 2004 Vol three.

Paulus, S., 2008, Implementing Criteria in the Production of Security Technology. Available at http://prise.oeaw.ac.at/docs/conf_docs/28/Paulus-Implementing_Privacy_Criteria-20080429.pdf.

Peissl, W., 2003, Surveillance and Security – a dodgy relationship., Journal of Contingencies and Crisis Management 11(1 March 2003), 19-24.

Privacy Commissioner of Australia, PIA Guide. Available at http://www.privacy.gov.au/publications/pia06/index.html.

Privacy Commissioner of Canada, Privacy Impact Assessment. Available at http://www.privcom.gc.ca/pia-efvp/index_e.asp

Raguse, M., 2007, PRISE - Privacy enhancing shaping of security research and technology, Deliverable 3.2 Evaluation Report. Available at http://www.prise.oeaw.ac.at/docs/PRISE_D3.2_Legal_Evaluation_Report.pdf.

Raguse, M., 2008, PRISE - Privacy enhancing shaping of security research and technology, Deliverable 3.3 Proposal Report. Available at http://www.prise.oeaw.ac.at/docs/PRISE_D3.3_Proposal_Report.pdf.

Rössler, B., 2003, Der Wert des Privaten, in: Grötker, R. (Hg.): Privat! Kontrollierte Freiheit in einer vernetzten Welt, 1. Aufl., Hannover: Heise Zeitschriften Verlag GmbH & Co KG, 15-32.

Schneier, B., 1999, Attack Trees, Dr. Dobbs Journal. Available at http://www.schneier.com/paper-attacktrees-ddj-ft.html.

Schumpeter, J., 1952, Theorie der wirtschaftlichen Entwicklung – Eine Untersuchung über Unternehmergewinn, Kapital, Kredit, Zins und den Konjunkturzyklus, 5. Aufl., Berlin: Duncker & Humblot.

Swoboda, P., 1984, Schumpeter's Entrepreneur in Modern Economic Theory, in: Seidl, C. (Hg.): Schumpeterian Economics – Schumpeter Centenary Memorial Lectures Graz 1983, Berlin/Heidelberg/New York/Tokyo: Springer, 17-30.

The Study Group on Europe's Security Capabilities, 2004, Human Security Doctrine for Europe. Available at http://www.lse.ac.uk/Depts/global/Publications/HumanSecurityDoctrine.pdf.

Thomas Hobbes, The Leviathan cit in: Taylor OWEN (2004) Challenges and opportunities for defining and measuring human security in HUMAN RIGHTS, HUMAN SECURITY AND DISARMAMENT, disarmanet forum 2004 Vol three.

Tretter, H. (ed.), 1984, KSZE. Die Abschlussdokumente der Konferenz für Sicherheit und Zusammenarbeit in Europa. 1975 und der Nachfolgekonferenzen Belgrad 1978 und Madrid 1983, Wien.

TÜV Informationstechnik GmbH, quid! - Das Qualitätszeichen für Datenschutz. Available at http://www.tuvit.de/47365.asp.

Ullman, R., 1983, Redefining Security, International Security, vol. 8, no. 1;

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens. Available at https://www.datenschutzzentrum.de/download/anford.pdf.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Datenschutzgütesiegel beim Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Available at https://www.datenschutzzentrum.de/guetesiegel/index.htm.

United Nations Development Programme, 1994, 'New Dimensions of Human Security', Human Development Report 1994, New York, Oxford University Press.

von Bredow, 2005, The Barcelona Report on a Human Security Doctrine for Europe, Overview and Some critical Remarks. Berlin Symposium on Human Security and EU-Canada Relations Canadian Universities' Centre Berlin March 3, 2005 Wilfried von Bredow Institut für Politikwissenschaft Philipps-Universität D-35032 Marburg

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

Weinandy, K., 2007, Sicherheitsforschung das Geschäft mit der Angst. Die Rolle der Ökonomie im (Un)Sicherheitsdiskurs – Eine kritische Betrachtung, Vienna: Unpublished manuscript.

Wikipedia, 2007, Security; Available at http://en.wikipedia.org/wiki/Security.

Zurawski, N. (ed.), 2007, Surveillance Studies Perspektiven eines Forschungsfeldes, Opladen: Verlag Barbara Budrich.