PASR

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

Grant Agreement no. 108600
Supporting activity acronym: PRISE

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

Activity type: Supporting Activity

Deliverable 3.2 Legal Evaluation Report

Final version April 2008

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

Author:
Maren Raguse, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

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

Partners

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

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

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

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

Table of Contents **page**

Executive Summary

This report presents an overview of legal requirements which lay down the scope of security technology use (national powers of investigation of a number of Member States are summarized) and of such provisions which deal with information sharing among Member States. As the level of privacy impact also depends on legal provisions, a product which might enable privacy compliant use may still be used in a far more infringing way than intended or foreseen by its developers, according to national police law. Also, national governments may ask for a customized technology, very often research is even triggered by demands of national governments acting as contractors. In this respect the same legislator who is entrusted with ensuring civil rights currently puts focus on national and international policy on preventing terrorism and organized crime by expanding police and secret service powers.

The European Court of Human Rights (ECHR) has dealt with the scope of privacy in the light of inner security measures. Relevant case law is presented.

Furthermore, the German constitutional court has ruled that the right to privacy embraces a core which must not be violated even for the purpose of safeguarding inner security. In this report the arguments of the court are be presented. The judgements are based on constitutional and fundamental rights which also exist in the European legal framework and are thus significant from a European perspective.

The purpose of this part of PRISE research is to categorize the known privacy impact of technical features in security technologies and make proposals for research resulting in privacy enhancing security technologies. PRISE does not analyze the compliance of existing applications and technologies with national laws. PRISE seeks to develop general criteria for funding of security research aiming at privacy compliant or even enhancing technologies within the Framework 7 programme.[1] This report does support this aim by giving an overview of the legal requirements applicable and of limits of privacy restrictions under the safeguarding of inner security exemption. In order to enable analogue application of the findings, they are based on general privacy principles derived from the OECD guidelines, the Data Protection Directive 1995/46/EC and Convention 108.

This report prepares the ground for the Proposal Report[2] which will present existing gaps in organisational, technical and legal dimensions with respect to privacy compliant security technologies and the research thereof.

The Proposal Report will describe which measures can and should be taken to ensure privacy enhancing security technologies. It will present options for privacy enhancing design of security technologies. The proposals will embrace the following three dimensions: technical features, legal framework and organisational embedding of a process to assure privacy compliance.

---

1 Seventh Research Framework Programme (FP7), http://cordis.europa.eu/fp7/home_en.html.

2 PRISE Deliverable 3.3 Proposal Report

The proposals will be directed at the FP 7 funding process and will also cover suggestions for possible changes in current legislation.

Chapter 1 Introduction

> *There are those who hope new technology can redress these invasions of personal autonomy that information technology now makes possible, but I don't share this hope. To be sure, it is possible and desirable to provide technical safeguards against unauthorized access. It is even conceivable that computers could be programmed to have their memories fade with time and to eliminate specific identity. Such safeguards are highly desirable, but the basic safeguards cannot be provided by new inventions.*
>
> *They must be provided by the legislative and legal systems of this country. We must face the need to provide adequate guarantees for individual privacy*[3].
>
> *– Jerome B. Wiesner, Science Advisor to President Kennedy –*

Since the September 11 attacks in 2001 the United States endorse the view of a raised threat by terrorists and have thus significantly amended their legislation allocating new and unprecedented investigative powers and powers of intervention to law enforcement and secret service authorities. Following terrorist attacks in Madrid and London also European governments have reacted by introducing or amending anti-terrorism laws. These legislative steps aim at detecting conspiracies to committing terrorist acts or other severe crimes at an early stage of planning. In order to achieve this early locating of terrorists and criminals the legislative measures seek to cover all areas of terrorist planning: Border control to prevent entry of known terrorists, detecting their communication, detecting their whereabouts and social networks, interrupting their cash flow and protecting potential targets like critical infrastructure or air travel.

The collection, maintenance, use, and dissemination of personal information by law enforcement authorities and secret services directly affect the privacy of individuals who are in the focus of criminal investigations. All of the aforementioned means of data processing are enabled by the use of technology. PRISE looks into technologies or means (systems, legislation etc.) which are intended to, or have a significant potential to, enhance the security of the society against threats from individuals, or groups of individuals.[4] While twenty years ago the means of stopping terrorism where old-fashioned tools like strict physical security at vulnerable facilities, intelligence gathering by government agents and vigilance on the part of all citizens, the 21st century knows a more sophisticated tool: advanced technology.[5] With ubiquitous technologies supporting and accelerating many aspects of personal and work life, we leave electronic traces every day: paying with our credit card, being captured by the shopping mall's CCTV, booking a flight, using the internet, calling a friend or business partner. The possible linkability of (electronically available) information from various sources is the main challenge to the right of informational self-determination.

---

[3] Testimony of Jerome B. Wiesner (1971) Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the House Committee on the Judiciary, 92d Congress of the United States.

[4] See PRISE Deliverable 2.2. Technology Report, Executive Summary.

[5] Ham, S. and Atkinson, R. D. (2002) Using Technology to Detect and Prevent Terrorism, Progressive Policy Institute Policy Brief.

In order to be in a position to detect plans of attacks early or enable a later analysis of networks and planning, European governments argue that it is necessary to collect information on individuals early (even without a sufficient suspicion of a criminal act such as it is for example the case with the Directive on Data Retention). In order to enable the collection of and access to more data on possible suspects or even to detect unknown suspects, new or changed rights cover eavesdropping of communication, access to information from commercial sources including banks or airlines, the introduction or expansion of DNA databases, the introduction of biometric passports and national ID-cards.

Furthermore, as terrorism is considered a global threat and terrorist networks cross national borders, the need for an increased exchange of information among EU Member States has been stated. The EU has addressed this issue at the 'Hague Programme' and put great emphasis on the exchange of data under the principle of 'availability' and in 2005 the Commission has adopted a proposal for a Council Framework Decision on the exchange of information under the principle of availability.

Outside the EU's institutions and legal framework, on 27 May 2005, seven Member States signed the Prüm Convention on adoption of cross-border cooperation. The focus of the cooperation is particularly on combating terrorism, cross-border crime and illegal immigration. It introduces inter alia measures to improve information exchange for DNA and fingerprints. The Contracting Parties had aimed to incorporate the provisions of the convention into the legal framework of the European Union. An according decision was passed by the council of European Union justice and home affairs ministers in February 2007.

Criminals and terrorists use state of the art technologies to disguise their traces, plans and communication more than ordinary citizens, and police and secret services need new or improved technologies to match this. It is for this reason that a focus of the EU's Framework 7 will be on security technologies.

The terms 'security' and 'security technologies' in the context of the PRISE work have been described in the 'Technology Report'[6] as follows: *Security* can be defined as the absence of danger – that is a state where the desired status quo is not threatened or disrupted in any way. In the context of the PRISE project, security is understood as the security of the society – or more precisely – of the citizens that constitute the society.

The term *security technology* can cover everything from private alarm systems and virus protection systems for PCs to border control systems and international police co-operation. In order to focus our work, the participants of the PRISE consortium have defined a set of criteria that security technologies and means should fulfil in order to be relevant to the project:

- The technologies or means (systems, legislation etc.) are intended to, or have a significant potential to, enhance the security of the society against threats from individuals, or groups of individuals (not from states). This covers crime-fighting, anti-terror activities, border control activities etc.

[6] PRISE Deliverable 2.2. Technology Report

- As focus is on the security of the society, we will not cover technologies that focus on protecting specific individuals or businesses, such as home alarm systems or security systems for computers and computer networks aimed at individuals and businesses.
- PRISE only discusses technologies that directly or indirectly may infringe the privacy of individuals.
- The technologies and means discussed are either existing technologies, technologies that are perceived to be important in the foreseeable future or that are part of on-going R&D projects.

The actual application of a security technology is determined by the national law of the Member States. Use of security technologies and the general definition of powers of intervention together with the used investigative methods in a specific investigation determine the level of privacy impact for citizens that are subject to the investigation or screening.

It has been claimed that Human Rights have been among the first casualties of the EU countries' efforts to strengthen their anti-terrorism powers.[7] From January 2007 until June 2007 Europe faced under the German EU Presidency a focus of the European discourse to be on the fight against terrorism, information system cross-referencing, and fighting cross-border crime by stepping up cross-border police cooperation.[8] While calls for extended information exchange and further investigative methods are numerous, a discussion on limiting of privacy impacts has not been widely brought up.

Article 13 of Directive 1995/46/EC states that the right to privacy may be restricted when such a restriction constitutes a necessary measure to safeguard public security and the prevention, investigation, detection and prosecution of criminal offences. In this context the question arises whether this allows for a state of 'zero privacy' or whether governments in their late legislative changes have indeed sought to strike a balance between privacy and security.

Security technologies must allow use compliant with general privacy principles which are a common ground for Member States due to transposition of Directive 1995/46/EC. Member States have to follow the principle of data minimization and must allow deletion and, if possible, anonymization and pseudonymization of personal data. Data collection and access has to be logged in a way that allows later scrutiny of the collection by a court of law. The quality of the data must be technically ensured, no altering of data collected as evidence must be possible. Only authorized access to collected data stored in databases must be possible. The aforementioned features are self-evident conclusions based on existing law and should be already implemented in all technologies which collect, process or transmit personal data. But companies developing security technologies do not always consider privacy aspects of their research. In fact, achieving privacy compliance or even enhancement may be seen as a hindrance for sketched new inventions, consuming financial and manpower resources while on the other hand the benefit of compliance seems unclear to them.

---

[7] Dick Oosting (2006) Europe's clampdown on terrorism risks backfiring. *Europe's World*, Spring 2006, pp. 131 – 137.

[8] 'Living Europe Safely' Work Programme of the Federal Ministry of the Interior for the German EU presidency (2007) can be found at http://www.statewatch.org/news/2007/jan/eu-counc-pres-prog.pdf .

Chapter 2 Legal Requirements

This chapter aims at giving a description of the regulations that cover the use of security technologies, as well as applicable privacy and data protection law in the context of measures aiming at safeguarding inner security. This section can only give an overview, as the instruments, requirements and especially the national provisions are too numerous to be presented for all EU member states.

Generally speaking, the parties involved in the data processing that occurs when security technologies are applied can be public authorities, citizens and companies. The addressees of police laws are public authorities who are allocated the competence to apply security technologies when preventing or investigating crimes. Citizens are obliged to tolerate these investigation measures. Privacy laws on the other hand do not differentiate between addressees and are directed at public authorities as well as companies or individuals as they transpose the Data Protection Directive which in Article 2 (d) lays down the definition of a data 'controller' who can be a 'natural or legal person, public authority, agency or any other body'. When security technologies are applied by law enforcement authorities, a complex system of legal provision applies to this situation.

This chapter will present an overview of regulations and declarations applicable to cross-border cooperation in criminal matters, actual powers of investigation as well as privacy protection.

The overview is divided into four sections. The first section 'International Instruments with regards to privacy' is describing provisions on an international and European level designed to protect privacy and data protection. The second section 'International Instruments with regards to criminal cooperation' presents provisions designed to enhance and harmonize law enforcements ability to capture and process personal information. Third, national data protection laws exist transposing the European data protection Directives. Fourth, national laws exist designed to support police powers. In addition, case law dealing with the restriction of privacy in order to safeguard security exists. Applicable case law is presented in the fourth chapter.

2.1 International Instruments with regards to privacy

The EU Member States are not only bound by the supranational law of the EU but also by international law. All Member States of the European Union are also members of the Council of Europe and the United Nations and have signed and ratified numerous international treaties, both dealing with human rights as well as joint anti-terrorism measures. On an international level the first steps with respect to ensuring privacy as a human right date back to 1950. Having ratified[9] the Convention for the Protection of Human Rights and Fundamental

[9] Simplified Chart of signatures and ratifications of EU Member States to Council of Europe human rights convention and protocols at http://conventions.coe.int/Treaty/Commun/ListeParGroupe.asp?GR=1&MA=3&CM=15&CL=ENG.

Freedoms, EU Member States are subject to the jurisdiction of the European Court of Human Rights.[10] A number of relevant cases for the work of PRISE will be presented in chapter 4.

Privacy in most western states is a constitutional right protected by explicit rules.[11] These provisions include rights of inviolability of the home and secrecy of communications at a minimum. If there is no explicit recognition of privacy in the constitution, states like Ireland, the United States or India draw that right from other provisions.

The first international regulation introducing a rule on the protection of privacy as a human right is article 12 of the Universal Declaration of Human Rights adopted in 1948 by the United Nations.[12] Almost the exact same wording is repeated in article 17 of the International Covenant on Civil and Political Rights the United Nations adopted in 1976. While this convention is binding law, the declaration on human rights is not legally binding for national law.[13]

The Council of Europe with its 46 member states adopted the European Convention for the protection of human rights and fundamental freedoms (ECHR) in 1950. The ECHR is a binding treaty. Article 8 of the ECHR lays down the right to respect for private and family life.[14] Article 6 (2) of the Treaty on European Union makes the European Union comply with the ECHR's fundamental rights.[15] In 1981 the Council of Europe adopted the Convention for the protection of individuals with regard to automatic processing of personal data, called Convention 108. On the 28th of January, the signing day of the Convention 108, the European Data Protection Day is held. The convention lays down basic principles for data protection in Articles 5 to 8:

Legitimacy: Personal data shall be obtained and processed fairly and lawfully.

Purpose binding: Personal data shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.

Proportionality: Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are stored.

---

[10] The website of the ECHR can be visited at http://www.echr.coe.int/ECHR/.

[11] Privacy International: Privacy and Human Rights – An International Survey of Privacy Laws and Practice, available at http://www.gilc.org/privacy/survey/intro.html. For an overview of European constitutional provisions on privacy see Council of Europe at http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/NATIONAlLAWS-EN.asp.

[12] *Universal Declaration of Human Rights*, Article 12: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.* See http://www.un.org/Overview/rights.html

[13] See for example Hans Peter Schmitz and Kathryn Sikkink (2001): *International Human Rights* at http://faculty.maxwell.syr.edu/hpschmitz/hpschmitz/ch27.pdf .

[14] ECHR Article 8: *Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

[15] Treaty on the European Union in the consolidated version of Nice (2002), available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/ce321/ce32120061229en00010331.pdf .

Quality of data: Personal data shall be accurate and, where necessary, kept up to date.

Linkability: Personal data shall be preserved in a form which permits identification of the data subject for no longer than is required for the purpose of which those data are stored.

Data Security: Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as unauthorized access, alteration or dissemination.

All EU Member States ratified this convention which lays down data protection as protection of fundamental rights and in particular the individual's right to privacy. They were thus required to implement the convention into their national laws. Convention 108 allows for the derogation of the basic principles in the interest of protecting state security, public safety or the suppression of criminal offences. Supplementing the convention in 2004 an additional protocol[16] went into force which concerns supervisory authorities and transborder data flows. Additionally, the Council of Europe has issued recommendations on a vast number of special areas of privacy law, for example the protection of personal data in the area of telecommunication services or the communication of personal data held by public bodies to third parties.[17]

Furthermore, the Organization for Economic Cooperation and Development (OECD) adopted the Guidelines on the protection of Privacy and Transborder Flows of Personal Data in 1980.[18] Only 19 of the 27 EU Member States are also member countries[19] of the OECD. Decisions-making power is held by the OECD's Council and decisions require a unanimous vote. The OECD guidelines of 1980 lay down a number of privacy principles which can also be found in the EU Data Protection directive of 1995. The OECD guidelines should be regarded as minimum standards.[20] These principles are:

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject (Part II, Paragraph 7).

Data Quality Principle: Personal data should be relevant for the purpose for which they are to be used, and, to the extend necessary for the purpose, should be accurate, complete and kept up-to-date (Part II, Paragraph 8).

Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use

---

[16] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (CETS No.: 181), available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=1&DF=1/23/2007&CL=ENG.

[17] For a list of recommendations and resolutions on privacy see http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international_legal_instruments/2CM.asp#TopOfPage .

[18] Available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[19] An overview of the OECD member states can be found at http://www.oecd.org/document/58/0,2340,en_2649_201185_1889402_1_1_1_1,00.html.

[20] Part I, Paragraph 6 of the guidelines.

limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose (Part II, Paragraph 9).

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except with the consent of the data subject or by the authority of law (Part II, Paragraph 10).

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data (Part II, Paragraph 11).

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller (Part II, Paragraph 12).

Individual Participation Principle: An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him data relating to him within reasonable time, at a charge - if any - that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; to be given reasons if a request is denied, and to be able to challenge such denial and to challenge data relating to him and – if the challenge is successful to have the data erased, rectified, completed or amended (Part II, Paragraph 13).

Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above (Part II, Paragraph 14).

The OECD guidelines are non-binding international law and the OECD member countries can choose to adopt equivalent national provisions or not to do so. On the contrary, ratification of the Council of Europe conventions results in the obligation to comply with these regulations.

The OECD Guidelines, the Convention 108 and the Data Protection directive 95/46/EC each mark a fundamental data protection instrument. Still, currently only the ECHR is enforceable[21] by an independent responsible court, the European Court of Human Rights.

In Europe and worldwide the first law on data protection was passed in the German *Land* of Hesse in 1970. Sweden was the next European country to follow with a law on data protection in 1973.[22] With more Member States enacting data protection and privacy laws and following Convention 108, the need for harmonization of this field of law relevant for the single European market was born.

---

[21] See also OECD (2006) report on the cross-border enforcement of privacy laws, available at http://www.oecd.org/dataoecd/17/43/37558845.pdf.

[22] Datalagen of 1973, Svensk Författningssamling (SFS) 1973, page 289.

Starting from the regulations of Convention 108 the European Commission adopted the Directive 95/46/EC (Data Protection) after four years of discussion and obliged the Member States to bring their legislation into line with the Directive. The Directive contains fundamental rules on the lawfulness of the processing of personal data as well as on the rights of the data subject.

It lays down a number of general principles of data protection:

Legitimacy: Personal data[23] must be processed[24] lawfully and the processing requires a legal basis or the consent of the data subject.

Proportionality: Personal data must adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

Purpose binding: Personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

Transparency: The data subject has to be aware of data processing taking place and of what data is being processed by which party. Rectification of inaccurate or incompetent data must be possible.

Quality of the data: The personal data collected shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data that is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

Security of the data: The controller shall implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.

Since 1995 further Directives in specific areas have been adopted. The Directive 2002/58/EC on privacy and electronic communication covers issues like security and confidentiality of communications, the storage of traffic data[25] and location data.

The European Commission has drafted a proposal for a framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM 2005(475)). The proposal aims at improving the judicial co-operation, in particular regarding the prevention and combating of terrorism. The Directive 95/46/EC (Data Protection) does not apply to activities that fall outside the scope of Community law such as the judicial co-operation in criminal matters.

In any case, Member States are under the obligation to have legislation in place to provide data protection for justice and home affairs to the standard of Convention 108.[26]

---

[23] See article 2 (a): "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject").

[24] See article 2 (b): "processing of personal data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

[25] Some provisions on the storage of traffic data were replaced by the Directive 2006/24/EC (data retention).

The treaty establishing a constitution for Europe did not enter into force as not all Member States ratified the treaty.[27] German Chancellor Angela Merkel put efforts of saving the EU constitution at the centre of the German European Union's Presidency in the first half of 2007.[28] Following the rejection of the European Constitution, the EU leaders agreed on a mandate for an Intergovernmental Conference in June 2007. The Intergovernmental Conference elaborated a draft reform treaty which was presented on the 19th of October 2007. This treaty aims at incorporating parts of the European Constitution by amending the Treaty on European Union and the Treaty Establishing the European Community.

Article II-67 of the rejected constitution laid down privacy as a fundamental right: *Everyone has the right to respect for his or her private and family life, home and communications.*

The protection of personal data was regulated in article II-68: *Everyone has the right to the protection of personal data concerning him or her.*

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

The draft reform treaty contains a reference to fundamental rights in the draft for a new Article 6 of the treaty of the European Union[29] and seeks to incorporate them as 'general principles' into the Union's law:

1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of 7 December 2000, as adapted [at…, on... 2007], which shall have the same legal value as the Treaties.
The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties.
The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.
2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.

---

[26] Article 14 of Convention Based on Article K.3 of the Treaty on European Union, on the Establishment of a European Police Office (Europol Convention) reads: *By the time of the entry into force of this Convention at the latest, each Member State shall, under its national legislation, take the necessary measures in relation to the processing of personal data in data files in the framework of this Convention to ensure a standard of data protection which at least corresponds to the standard resulting from the implementation of the principles of the Council of Europe Convention of 28 January 1981, and, in doing so, shall take account of Recommendation No R(87) of the Committee of Ministers of the Council of Europe of 17 September 1987 concerning the use of personal data in the police sector.*

[27] After two referendums rejecting the ratification in the Netherlands and France the constitution cannot enter into force as it needs a unanimous vote. For an overview of the current status of the 'Institutional Reform of the European Union' see http://europa.eu/institutional_reform/chronology/index_en.htm .

[28] International Herald Tribune (January 2007) Constitution and trade at top of Merkel's EU agenda, available at http://www.iht.com/articles/2007/01/17/news/europe.php .

[29] The draft reform treaty is available at http://www.consilium.europa.eu/uedocs/cmsUpload/cg00001re01en.pdf

3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.

As described before, Article 8 of the ECHR lays down the right to respect for private and family life. Already now, Article 6 (2) of the Treaty on European Union makes the European Union comply with the ECHR's fundamental rights. Hence, an explicit incorporation of the right to privacy or private life, as laid down in the rejected Constitution, into the Treaty on European Union is currently not planned.

2.2 International Instruments with regards to criminal cooperation

The European Union unites the three pillars of the European cooperation. The European Community (EC) serves as the first pillar which covers economic, social and environmental policies. Decisions in the first pillar are subject to supranational law. The second and third pillars were established under the Treaty of the European Union. They are concerned with the common foreign and security policy and justice and home affairs and decisions are made intergovernmental.

The first pillar comprises of the three European Communities and embodies Community jurisdiction. Within the framework of the EC, the institutions of the Community may draw up legislation in the respective areas of responsibility that applies directly to the Member States. Art. 249 of the treaty establishing the European Community provides several tools to the Community institutions to regulate European law: regulations, directives, decisions and recommendations.

The Common Foreign and Security Policy (CFSP) makes up the second pillar and is regulated in Art. 11 - 28 of the treaty on the European Union. The Police and Judicial Co-operation in Criminal Matters (PJCC) makes up the third pillar and is regulated in Art. 29 - 42 of the treaty on the European Union. The three pillar-structure of the European Union results from the negotiations leading up to the Maastricht treaty and is reflected in the structure of the treaty on the European Union.

Within the second and third pillar the European Community has no express or implied powers and jurisdiction is mostly intergovernmental. Decisions on common foreign- and security policy are taken on the basis of cooperation between the Member States. Tools in the context of this intergovernmental practice are for example decisions of principle, joint actions, common positions or framework decisions. Framework decisions can be compared to an EU directive. In May 2005 seven Member States signed an international treaty, the Prüm Convention, on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration.[30] It introduces measures to extend information exchange for DNA and fingerprints. The Convention is open for all Member States of the European Union to join. The contracting Member States aim to incorporate the provisions of the Prüm Convention into the legal framework of the European Union. The Prüm Convention aims at implementing the principle of availability as set out in the Council

[30] As published by Statewatch at http://www.statewatch.org/news/2005/aug/Pr%FCm-Convention.pdf .

Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final) on an intergovernmental level. The EU JHA Council agreed on incorporating the main provisions of the Prüm Convention into the EU's legal framework on 15 February 2007. An according council decision on the stepping up of cross-border co-operation[31] was adopted on 12 June 2007.[32]

The Council of Europe has adopted a number of conventions and amending protocols dealing with anti-terrorism measures. The first Convention on the Suppression of Terrorism was adopted in 1977[33] and a protocol amending the convention was adopted in 2003[34]. Further instruments adopted by the Council of Europe include the European Convention on Extradition[35], the European Convention on Mutual Assistance in Criminal Matters[36], the European Convention on the transfer of proceedings in Criminal Matters[37], the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime[38], the Convention on Cybercrime[39], the Council of Europe Convention on the Prevention of Terrorism[40] and the Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and the financing of terrorism[41]. The Council of Europe Convention on the Prevention of Terrorism of 2005 aims at the implementation of measures that may be necessary to improve and develop the co-operation among national authorities in order to prevent terrorist offences. This includes the exchange of information and improving the physical protection of persons and facilities.

In addition, the Committee of Ministers, the Council of Europe's decision-making body, has made several recommendations dealing with a joint fight against organised crime and terrorism. Recommendations are not binding to the member States. Recommendation Rec (2005) 10[42] is particularly relevant to look into for the PRISE project. It recommends general principles for the use of special investigation techniques at a national level. The definition given for the term 'special investigation techniques' is broad and shall cover techniques

---

[31] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/803&format=HTML&aged=0&language=EN&guiLanguage=en

[32] Press release of German EU Presidency at http://www.eu2007.de/en/News/Press_Releases/February/0215BMIPruem.html.

[33] European Convention on the Suppression of Terrrorism (ETS 90) (1977), available at http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/ETS%2090.pdf.

[34] Protocol amending the European Convention on the Supression of Terrorism (ETS 190) (2003), available at http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=190&CM=8&DF=2/12/2007&CL=ENG.

[35] European Convention on Extradition, (ETS 24) (1957), available at http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=024&CM=8&DF=2/12/2007&CL=ENG.

[36] European Convention on Mutual Assistance in Criminal Matters (ETS 30) (1959), available at http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=030&CM=8&DF=2/12/2007&CL=ENG.

[37] European Convention on the Transfer of Proceedings in Criminal Matters (ETS 73) (1972), available at http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=073&CM=8&DF=2/12/2007&CL=ENG.

[38] European Convention on Laundering, Search, Seizure and Confiscation on the Proceeds from Crime (ETS 141) (1990), available at http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=141&CM=8&DF=2/12/2007&CL=ENG.

[39] Convention on Cybercrime (ETS 185) (2001), available at http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=2/12/2007&CL=ENG.

[40] Council of Europe Convention on the Prevention of Terrorism (CETS 196) (2005), available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=8&DF=&CL=ENG.

[41] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds form Crime and on their Financing of Terrorism (CETS 198) (2005), available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=&CL=ENG.

[42] Recommendation REC(2005)10 of the Committee of Ministers to member states on „special investigation techniques" in relation to serious crimes including acts of terrorism, available at http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/fight_against_terrorism/2_adopted_texts/rec_2005_10E.pdf.

applied by law enforcement authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person. The recommendation thus deals with covert investigation methods such as bugging, eavesdropping, surveillance of telecommunications, the linking and mining of data from several (commercial or government) databases. It can therefore be applied to many technologies described in the PRISE Technology Report[43], in particular to those aiming at investigation prior to an act of crime that the law enforcement authorities have no distinct knowledge of. The recommendation includes the following principles:

- Member states should take appropriate legislative measures to allow the use of special investigation techniques with a view to making them available to their competent authorities to the extend that is *necessary* in a democratic society and is considered *appropriate* for efficient criminal investigation and prosecution.

- Member states should take appropriate legislative measures to ensure adequate control of the implementation of special investigation techniques by judicial authorities or other independent bodies through prior authorisation, supervision during the investigation or ex post facto review.

- Special investigation techniques should only be used where there is sufficient reason to believe that a *serious crime* has been committed or prepared, or is being prepared, by one or more *particular* persons or an as-yet-unidentified individual or group of individuals.

- Proportionality between the effects of the use of special investigation techniques and the objective that has been identified should be ensured. In this respect, when deciding on their use, an *evaluation* in the light of the seriousness of the offence and taking into account the intrusive nature of the specific special investigation technique used should be made.

- Member states should ensure that competent authorities apply *less intrusive* investigation methods than special investigation techniques if such methods enable the offence to be detected, prevented or prosecuted with adequate effectiveness.

- Member states should in principle, take appropriate legislative measures to permit the *production of evidence* gained from the use of special investigation techniques before courts.

- Member states should ensure that, with respect to those special investigation techniques involving technical equipment, *laws and procedures take into account* the new technologies. For this purpose, they should work closely with the private sector to obtain their assistance in order to ensure the most effective use of existing technologies used in special investigation techniques and to maintain effectiveness in the use of new technologies.

[43] PRISE Deliverable 2.2 Overview of Security Technologies

- Member states should ensure, to an appropriate extent, retention and preservation of traffic and location data by communication companies, such as telephone and Internet service providers, in accordance with national legislation and international instruments, especially the European Convention on Human Rights and the Convention 108.

- Member states should take appropriate measures to ensure that the technology required for special investigation techniques, in particular with respect to interception of communications, meets *minimum requirements* of confidentiality, integrity and availability.

- Member states should ensure adequate *training* of competent authorities in charge of the decision to use, supervision and use of special investigation techniques.

This Recommendation of the Committee of Ministers indicates an important conclusion: the level of privacy impact of a criminal investigation enabled and carried out by use of security technologies is determined by three factors, each of which can be disproportionate or otherwise illegal and therefore has to be taken into account when assessing the privacy impact of a specific security technology application: These are the technical features of the technology, legal provision on investigation method and use of security technology, and the actual use of security technology in a specific investigation. In chapter 2.3 we will look more closely at these factors and suggest some minimum principles for minimum privacy standards that can be applied to them..

On an international level the ICAO (International Civil Aviation Organization) standards deal with technical specifications of machine readable travel documents. These standards have been adopted by the EU Commission Decisions on technical specifications of travel documents in Member States (C(2005) 409 and C(2006) 2909). Other specific technical requirements for security applications do currently not exist.

Generally speaking, rules on law enforcement practices and obligations, and thus the application of security technologies by law enforcement authorities, are still regulated within the national law. Crime fighting methods, like video surveillance, covert surveillance of tele-communications and private premises, the use of location technologies or DNA databases are regulated in national law.

Regulations on a European – supranational – level with regards to the application of security technologies by law enforcement authorities exist only for issues that arise in areas the European Community has jurisdiction in. The Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States for instance, was to lay down rules giving effect to the Convention implementing the Schengen Agreement.[44] Also provisions on the border and control visa information systems SIS (Schengen Information System), SIS II and VIS (Visa Information System) are regulated on a European level.

---

[44] Protocol 2 annexed to the Treaty on European Union integrates the Schengen acquis into the framework of the European Union. For the Schengen Agreement see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML.

Furthermore, the proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final) aims at establishing rules to ensure that information needed for the fight against crime should cross the internal borders of the EU without obstacles. The principle of availability that the Commission aims at regulating means that information that is available to certain authorities in a Member State must also be provided to the equivalent authorities in other Member States. The proposed Council Framework Decision follows the same goal as the Prüm Convention. The exchange of law enforcement information includes sensitive data like fingerprints or DNA information.

At the beginning of 2006 the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks was adopted. The Directive regulates the scope of the retention of traffic and location data in the Member States in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

Previous to the new directive traffic and location data had to be erased when it was no longer needed for the purpose of the transmission of a communication, respectively after the duration necessary for the provision of a value added service. Processing of traffic data was permissible only to the end of the period during which the bill could lawfully be challenged or payment pursued. The new directive extends the period of storage until not less than six months and not more than two years from the date of the communication.

The Member States Ireland and Slovakia have issued a legal challenge to the Directive 2006/24/EC at the European Court of Justice (ECJ) claiming the wrong legal basis was chosen for the Directive.[45]

Legal provisions are in place in Member States regulating the scope of police powers of intervention. These statutes provide the legal basis for the use of a certain type of technology (like monitoring of telecommunications or audio-visual monitoring of individuals) but do not lay down specific provisions on the exact way to use a specific technology nor do they specify technical features of security technologies.

General provisions laid down in Directive 1995/46/EC apply also to security technologies. Article 17 states that Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

On an EU level, the Commission decisions[46] regarding the technical specifications on the standards for security features and biometrics in passports and travel documents issued by member states have established a framework for machine readable travel.

---

[45] The European Court of Justice ruled in May 2006 that the Agreement between the European Community and the United States of America on the Passenger Name Records of air passengers transferred to the United States was based on a wrong legal basis and annulled the respective Decisions. The data was initially collected for a purpose that falls under Community law (the purchase of an airline ticket) while the transfer for the purpose of safeguarding public security falls within a framework on public security. The Directive 2006/24/EC changes the purpose of data storage from providing a communication service to enabling the investigation, detection and prosecution of serious crime.

2.3 Minimum privacy standards in national data protection laws: general principles

European Data Protection law is harmonized by the European Directives 1995/46/EC and 2002/58/EC. These national data protection laws must follow the same principles laid down in the Directives as well as further international instruments. In order to receive an easy to handle set of minimum standard, for the purpose of further criteria definition PRISE will analyse technologies and to be developed criteria by means of mapping against the following common principles on a European Level. A profound analysis will always have to take into account the applicable national provisions.

These principles set out in the OECD guidelines, the Convention 108 and the Data Protection Directive can be merged to a set of principles summarizing all of these sources:

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

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

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

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

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

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

While PRISE draws basic privacy principles from the existing international and European regulatory frameworks, a detailed analysis would always have to include the applicable national regulations, too. The national provisions provide the exact purpose of data collected and further processed by law enforcement authorities and a use of security technologies according to these national provisions may, depending on their definition, violate the proportionality principle or the purpose binding principle. For the purpose of this legal analysis, the above listed principles are regarded a common minimum standard of privacy requirements. All Member States have to provide a level of protection of privacy as laid down in Directive 1995/46/EC, Directive 2002/52/EC and Convention 108, as transposition is implied. Furthermore, a detailed legal analysis can be carried out only with respect to an existing use case applying the actual national legal framework.

As Directive 1995/46/EC allows for the restriction to privacy when such a restriction constitutes a necessary measure to safeguard national security, defence, public security and the

---

[46] C (2006) 2909 and C (2005) 409.

prevention, investigation, detection and prosecution of criminal offences, a closer look at what this exemption means with respect to the privacy principles is necessary.

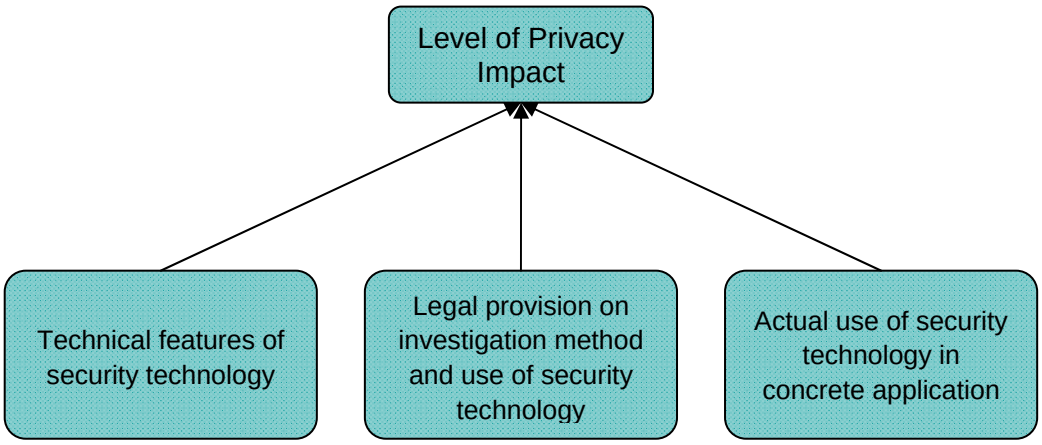

Figure 1: Determining factors for privacy impact

The level of privacy impact of a criminal investigation or preventive police measures enabled and carried out by use of security technologies is determined by three factors, each of which can be disproportionate or otherwise not compliant with legal regulations or fundamental rights. These factors are the technical features of the technology, the existing provisions regulating their application and finally the actual application in the cause of an investigation.

Each of these three dimensions' design can be non-compliant with privacy law, even though the right to privacy can be restricted to safeguard criminal investigations. The security technology's design must comply with provisions on technical features, in particular data security and data minimization. This means adequate technical protection of all forms of data processing (collection, disclosure, storage and alignment) must be implemented. The data security principle is fully applicable also to data processed in the cause of criminal investigations. It seems unlikely that assuring the security of data collected and further processed in the cause on an investigation by technical means like encryption should have a negative impact in an investigation. On the contrary: Protecting the data against loss or alteration will even increase the data's suitability for further use in the cause of the investigation as well as allowing thorough judicial scrutiny. In addition, the approach when defining the functionality of a technology must be to focus on finding the technical solution requiring as little data of as few people as possible and storing it for as short as possible to increase the technologies suitability for a proportionate use. Furthermore, if it is possible to

achieve the intended investigation result when first upholding anonymity and lifting it only if a hit occurs, anonymity then should be implemented to protect not suspicious data subjects[47].

In many criminal investigations covert technology use and covert investigation is a necessary approach to detect, prevent or investigate planned or committed criminal acts. In such a case, revealing the fact that an investigation is ongoing will jeopardize the result of the investigation. The remote and unobserved collection of data at the same time is very intrusive because the data subject is unaware of being subject to a criminal investigation. Such operations are clearly in contradiction to the transparency principle. It is for this reason that most covert investigative methods require a judicial order. Furthermore, in order to allow later judicial scrutiny, the data subject should be notified of the application of a covert investigative method as soon as the investigation is no longer obstructed by this. A current development is to process data from several (also commercial) sources to find possible connections of a suspect to other potential criminals.

The least intrusive means leading to an adequate result of the investigation must be chosen to ensure proportionality of the application. In other words, if an equivalent investigation result can be effectuated with less intrusive technological means these must be preferred. The proportionality principle is valid even under the restriction of privacy to safeguard inner security and criminal investigation exemption as its very purpose is to prevent excessive use of state power and arbitrariness. This objective applies precisely when measures that infringe fundamental rights are to be applied by public authorities. It is in many situations necessary for a state to interfere with citizens' fundamental rights in order to achieve legitimate purposes of public interest such as the maintenance of public order, or public safety. Yet, in doing so the citizens' individual rights must be protected as well as possible.

Before introducing new security technologies and regulations on their use, a necessary step is to consider how effective they are. Governments are not only the guardians of the inner security of a state, but also of the fundamental rights of their citizens. It is therefore important that they encourage the development of least intrusive and effective technologies.

The introduction of new legal provisions should follow an assessment of the effectiveness of the planned measure in relation to the associated fundamental rights intrusion, to ensure that the principle of proportionality is met. A later review of whether the expected boost to investigative measures has resulted from a newly adopted law, an evaluation of the law should be carried out to ensure that ineffective and at the same time very intrusive measures don't prevail.

Finally, the use of a security technology in the cause of a specific investigation must comply with the proportionality principle, too.

---

[47] See for example D. Agrawal and C. Aggarwal (2001) On the Design and Quantification or Privacy Preserving Data Mining Algorithms, available at http://citeseer.ist.psu.edu/cache/papers/cs/25580/http:zSzzSzweb.mit.eduzSzcharuzSzwwwzSzprivate.pdf/agrawal01design.pdf and L. Sweeney (2002) *k*-Anonymity: a model for protecting privacy, available at http://privacy.cs.cmu.edu/dataprivacy/projects/kanonymity/index.html. and K. Liu (2006) Privacy Preserving Data Mining Bibliography, available at http://www.csee.umbc.edu/~kunliu1/research/privacy_review.html .

2.4 Overview of Anti-Terrorism Legislation and Police Law of selected Member States

The overview of Legal Requirements in Chapter 2 of this report finally presents national legislation of selected Member States of the European Union aiming at preventing and detecting terrorism. Spain and Great Britain have been chosen as both countries faced terrorist attacks and thus an expectation would be that in a response to these attacks, new measures have been introduced aiming at preventing terrorist attacks. Austria was chosen to represent a Member State where no attack has occurred. As this section aims only at giving an overview of new responses to terrorist threats which involve use of new technologies, not all Member States are presented. Anti-terrorism legislation enables the detection of other serious crimes, too, and very often this term is in fact used as a synonym for laws extending investigative powers, data collection and data sharing by law enforcement authorities.

2.4.1 Austria

The Penal law of Austria is laid down in the Austrian Penal Code[48]. The Procedural rules are regulated in the Austrian Code of Criminal Procedure[49]. One of the most important recent amendments to Austrian Penal law, the Penal Law Amending Act 2002[50] has broadened the scope of the Penal Code with respect to preventing and detecting terrorism.[51] Furthermore, the Criminal Procedures Reform Act will enter into force by 1 January 2008 and will completely restructure the pre-trial phase of criminal proceedings.

The following provisions of the Penal Code might apply with respect to terrorist acts: murder[52], intentional bodily harm[53], criminal offences against personal liberty[54], damage to property[55], offences which are a threat to the public[56] (for instance arson, hijacking and wilful interference with the safety of aviation, endangering by nuclear energy, ionising radiation or explosives), money laundering[57], establishing a or being a member of a criminal association[58], leading or being a member of a terrorist association[59], and financing of terrorism[60].

Austrian jurisdiction applies to all criminal acts committed on Austrian territory and which are punishable according to Austrian Law.

The same legal provisions of the Austrian Code of Criminal Procedure apply before or during a trial against an individual suspected of criminal acts related to terrorism as they do to all

---

[48] Strafgesetzbuch; abbreviated: StGB.

[49] Strafprozessordnung; abbreviated: StPO.

[50] Strafrechtsänderungsgesetz 2002; Federal Law Gazette I No. 134/2002.

[51] Council of Europe Committee of Experts on Terrorism (CODEXTER) (2005) Profiles on Counter-Terrorism Capacity: Austria.

[52] Section 75 Penal Code.

[53] Sections 83 et seqq. Penal Code.

[54] Sections 99 et seqq. Penal Code.

[55] Sections 125 et seqq. Penal Code.

[56] Sections 169 et seqq. Penal Code.

[57] Section 165 Penal Code.

[58] Section 278 Penal Code.

[59] Section 278b Penal Code.

[60] Section 278d Penal Code.

suspected criminals.[61] Responding to the September 11 attacks in the United States, the government announced a package of measures to fight money laundering and terrorism on 15 October 2001.

In the context of terrorism the Austrian Code of Criminal Procedure allows for a number of investigation methods which represent a restriction of fundamental rights: provisions on search of a house or a person[62], seizure[63], search and seizure of documents[64], seizure and opening of letters and other items to be delivered[65], provisions on obligations to give evidence concerning bank accounts[66], monitoring of telecommunications[67], audio-visual monitoring of individuals by technical means[68] and computer-aided data cross-referencing[69]. An amendment to the Police Law[70] went into force in 2005 and empowers the police to keep public places under audio and video surveillance and to store the data collected up to 48 hours, or longer if there is a suspicion that a criminal offence was conducted.[71]

Most of the investigation methods stated above have to be ordered by an investigative judge upon request by the public prosecutor, while very intrusive methods of investigation like the monitoring of telecommunications, the audio-visual monitoring of individuals by technical means and the computer-aided data cross-referencing require a warrant issued by a chamber comprised of three judges.

Further requirements need to be fulfilled for the search of a domicile to be legally allowed. A house search may only be conducted if a reasonable suspicion that the person being suspected of an offence is hidden in the house or that there are objects whose detection could be important for the specific investigation.

Furthermore, audio-visual monitoring by technical means and computer-aided data cross referencing may only be conducted based on a court order issued by a chamber of three judges and based on a suspicion of a criminal act which is punishable by more than ten years of imprisonment. The investigation method must comply with the principle of proportionality in the specific investigation.

2.4.2 Spain

Spain is among the European countries which have been facing bomb attacks fuelled by national history for decades. It thus had, even before the September 11 attacks in 2001, anti-terrorism legislation in place and preventing and prosecuting terrorism has been a top priority

---

61 CODEXTER (2005): Austria.
62 Sections 139 et seqq. Code of Criminal Procedure.
63 Sections 143 et seqq. Code of Criminal Procedure.
64 Section 145 Code of Criminal Procedure.
65 Sections 146 et seqq. Code of Criminal Procedure.
66 Section 145a Code of Criminal Procedure.
67 Sections 149a et seqq Code of Criminal Procedure.
68 Sections 149d et seqq. Code of Criminal Procedure.
69 Sections 149i et seqq. Code of Criminal Procedure.
70 Sicherheitspolizeigesetz, SPG.
71 Section 54 (6) SPG.

for the Spanish government.[72] The Spanish Constitution lays down the fundamental right to privacy, inviolability of the domicile, secrecy of communications and the protection of personal data in Article 18.[73]

After the terrorist bombing in Madrid on 11 March 2004 Spain has adopted further anti-terrorism measures. A National Centre for Antiterrorist Coordination (CNCA) was set up and it exclusively aims at improving the fight against terrorism. Furthermore the Executive Committee for the State Law Enforcement Agencies Unified Command was set up and it seeks to improve the prevention and prosecution of crime in general, including terrorism. The recently created Intelligence Centre against Organised Crime (CICO) is responsible for developing an intelligence strategy for a fight against all kind of organised crime.

The Spanish legal framework applicable for the prevention and prosecution of terrorism is the same as for all other crimes. The main legal acts include the Spanish Constitution, The Penal Code, the Code of Criminal Procedure, Law 19/1993 covering anti money-laundering provisions, Law 11/2003 regulating joint intelligence units with the EU, Law 19/1994 on the prevention and freezing of terrorist financing and Organic Law 15/1999 on personal data protection. In May 2003 Law 12/2003 on preventing and freezing terrorist funding was adopted. Financial entities such as banks, credit entities or exchange bureaus are obliged to collaborate in providing all information required to further investigate the context of frozen funds. In November 2005 the National Defence Law was passed.[74] The law expanded the scope of investigation measures of the Spanish secret service agency 'National Intelligence Centre', introducing the right to 'contribute […] in obtaining, evaluating and interpreting the necessary information to prevent and avoid any risk or threat that affects the independence and integrity of Spain, national interests and the stability of the State of law and its institutions'.[75] Supplementing this Act is Law 19/2003 of July 2003 and which regulates the movement of money and international transactions and modified Law 19/1993 (anti money-laundering).

Articles 571 et seqq. of the Spanish Penal Code cover terrorist offences whereby belonging to, acting for the sake of, or collaborating with armed bands, bodies or groups whose aim lies in subverting the peace, by committing the following offences: destruction or arson, causing death or injuries, kidnapping, detaining a person unlawfully, under threat or coercion, or any other criminal offence.[76]

A trial against a suspect of a terrorist offence follows the same rules as a trial against any other suspect.

---

[72] Council of Europe Committee of Experts on Terrorism (CODEXTER) (2005) Profiles on Counter-Terrorism Capacity: Spain.

[73] For an English translation see http://www.congreso.es/ingles/funciones/constitucion/const_espa_texto.pdf .

[74] The amendment law 'Ley Orgánica 5/2005 de 17 de Noviembre' can be accessed here http://www.mde.es/contenido.jsp?id_nodo=4340&&&keyword=&auditoria=F .

[75] Translation taken from EPIC and Privacy International (2005) Privacy & Human Rights 2005: An International Survey of Privacy Laws and Developments, page 944. Available at http://www.privacyinternational.org/survey/phr2005/PHR2005swed-ven.pdf .

[76] Translation cited from Council of Europe Committee of Experts on Terrorism (CODEXTER) (2005) Profiles on Counter-Terrorism Capacity: Spain.

The Spanish legal system provides a number of investigative methods which impact fundamental rights[77] granted by the Spanish Constitution. Entry and search of a domicile are lawful only if there are clues that the suspect, the instrumental means to the offence, or any other object to be used for its prosecution or investigation, are to be found within the house. In addition to the aforementioned requirement, a search may only be conducted based on the consent of the owner, a court order or if a crime is just being committed.

For a restriction of the right to privacy of telecommunications a court order is needed. An exception to this general principle is stated in Article 579.4 of the Law of Criminal Procedure, whereby in case of an emergency, the Minister of the Interior may order the interception of telecommunications, if the investigation aims at uncovering actions relating to activities of armed bands or terrorists.

2.4.3 United Kingdom

The UK has been faced with attacks in connection with the Northern Ireland conflict for many years. Its counter terrorism efforts have been strengthened in recent years.[78]

The United Kingdom does not have a written constitution. The European Convention on Human Rights has been partly incorporated into domestic law by the Human Rights Act 1998.[79] This includes the incorporation of the right to privacy as a fundamental right.[80] The European Data Protection Directive 1995/46/EC was transposed into domestic law by the Data Protection Act 1998.[81]

The UK legal framework deals with a number of terrorist offences[82], but suspected terrorists are in general prosecuted under general criminal law offences such as crimes against the person, causing explosions or hostage taking.

Counter terrorist legislation in the UK includes the Terrorism Act 2000[83], the Anti-Terrorism, Crime and Security Act 2001[84], the Prevention of Terrorism Act 2005[85] and the Terrorism Act 2006[86]. Legal provisions on police and secret service measures are regulated in the Police and Criminal Evidence Act of 1984[87], the Criminal Justice Act 1988[88], Police Act 1996[89], the Criminal Justice and Police Act 2001[90], the Criminal Justice Act 2003[91], the Regulation of

---

77 This includes the right to inviolability of the domicile and the right to privacy of telecommunications.

78 Council of Europe Committee of Experts on Terrorism (CODEXTER) (2005) Profiles on Counter-Terrorism Capacity: United Kingdom.

79 Available at http://www.opsi.gov.uk/acts/acts1998/19980042.htm .

80 EPIC and Privacy International (2005) Privacy & Human Rights 2005: An International Survey of Privacy Laws and Developments, page 722. Available at http://www.privacyinternational.org/survey/phr2005/PHR2005swed-ven.pdf .

81 Available at http://www.opsi.gov.uk/acts/acts1998/19980029.htm .

82 Among them are funding of and support of terrorist groups or activities.

83 Available at http://www.opsi.gov.uk/acts/acts2000/20000011.htm .

84 Sections 89 to 107. Available at http://www.opsi.gov.uk/ACTS/acts2001/20010024.htm .

85 Available at http://www.opsi.gov.uk/acts/acts2005/20050002.htm .

86 Available at http://www.opsi.gov.uk/acts/acts2006/20060011.htm .

87 Available at http://police.homeoffice.gov.uk/operational-policing/powers-pace-codes/pace-code-intro/ .

88 Available at http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880033_en_1.htm .

89 Available at http://www.opsi.gov.uk/acts/acts1996/1996016.htm .

90 Available at http://www.opsi.gov.uk/acts/acts2001/20010016.htm .

Investigatory Powers Act (RIPA) 2000[92] and the Intelligence Service Act 1994[93]. Information sharing and data matching among public authorities was extended by the Crime and Disorder Act 1998.[94] The UK operates the world's largest DNA database which by the end of 2005 held 3.5 million DNA profiles (5,2 % of the UK population).[95] Regulations allow for DNA and fingerprints to be kept even if the data subject was not convicted of a crime and even DNA of juveniles[96] is kept in the UK National DNA Database. The UK DNA data has been reported to be shared with foreign law agencies on request.[97] All 519 requests from 2004 were granted. Despite of this willingness to share DNA data with other countries' law enforcement authorities Great Britain opposes joining the Prüm Convention.[98] In 2006, Prime Minister Blair called for the national DNA database to be expanded to include every citizen.[99]

The UK operates the largest number of CCTV cameras in Europe, up to 4.2 million cameras or one for every fourteen people.[100] While originally the purpose of installing camera networks was crime prevention, the systems are now also used for city center management and the control of 'anti-social behaviour'.[101] CCTV is used for motorist surveillance with automatic number plate recognition (ANPR) and existing high street and town centre cameras are called for to be integrated where possible.[102]

Investigation methods are mainly regulated in The Regulation of Investigatory Powers Act 2000. Covered investigation methods include interception of communications[103], acquisition and disclosure of communications data[104], covert surveillance[105] including bugging. Authority to place a bug in someone's domicile or vehicle is required from a Senior Officer and then by an independent Surveillance Commissioner, sections 32-40 RIPA. The RIPA has been criticised among others by the Information Commissioner because some of its provisions are

---

91 Available at http://www.opsi.gov.uk/acts/acts2003/20030044.htm .

92 Available at http://www.opsi.gov.uk/acts/acts2000/20000023.htm .

93 Available at http://www.opsi.gov.uk/ACTS/acts1994/Ukpga_19940013_en_1.htm .

94 Available at http://www.opsi.gov.uk/acts/acts1998/19980037.htm .

95 The Home Office on the national DNA database at http://www.homeoffice.gov.uk/science-research/using-science/dna-database/ and Parliamentary Office of Science and Technology (2006) Postnote – The national DNA database, available at http://www.parliament.uk/documents/upload/postpn258.pdf .

96 BBC (January 2006) Juveniles' DNA recording defended, available at http://news.bbc.co.uk/1/hi/uk/4633918.stm .

97 BBC (June 2006) DNA database is shared overseas, available at http://news.bbc.co.uk/1/hi/uk_politics/5056450.stm .

98 International Harald Tribune (January 2007) Germany seeks to modernize policing across Europe, available at http://www.iht.com/articles/2007/01/15/news/germany.php .

99 The Telegraph (October 2006) DNA database 'should include all', available at http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/10/24/ndna24.xml .

100 The Surveillance Studies Network (2006) 'A Surveillance Society' , available at http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_report.aspx .

101 EPIC and Privacy International (2005) Privacy & Human Rights 2005: An International Survey of Privacy Laws and Developments, page 731.

102 Clive Norris (2006) A Report on the Surveillance Society: Criminal Justice, available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_appendices_06.pdf

103 Chapter I of Part I of The Regulation of Investigatory Powers Act 2000.

104 Chapter II of Part I of The Regulation of Investigatory Powers Act 2000.

105 Part II of The Regulation of Investigatory Powers Act 2000 differentiates two types of covert surveillance: directed and intrusive surveillance. In the cause of an directed surveillance police or other authorities follow an individual in public and record their movement whereby an intrusive surveillance involves the presence of an individual on private residential premises or in a private vehicle and may involve the placing of bugs in cars and any interference with property.

regarded to violate the ECHR.[106] Several codes and regulations concerning the RIPA have been issued by the Home Office.[107]

The Prevention of Terrorist Act 2005 allows for the imposition of control orders upon individuals believed to be involved in terrorist-related activity. These preventative orders are controversial in the UK.[108] By means of a control order obligations may be imposed upon an individual and the range of possible obligations is vast. A control order can place restrictions on what the individual can use or may posses, his place of work, place of residence, whom he may speak to and where he may travel. Furthermore, a control order can order the electronic tagging of an individual in order for his movements to be tracked. The Home Secretary is required to make a statement to Parliament every three months reporting about his exercise of the control order powers.

2.4.4 Conclusion

The legal provisions on the powers of law enforcement authorities differ in EU Member States. A joint development is the extension of existing powers in member states, following a newly regarded need for anti-terrorism measures.

The following figure presents a general classification of common investigative methods according to the existing level of specific suspicion.

[106] The Guardian (July 2002) Blunkett security laws may be illegal available at http://politics.guardian.co.uk/homeaffairs/story/0,11026,766563,00.html and Foundation for Information Policy Research FIPR (2003) Communications surveillance briefing, available at http://www.fipr.org/030818ripa.html .

[107] For an overview see the Home Office's website at http://security.homeoffice.gov.uk/ripa/legislation/ripa-statutory-instruments/?version=1 .

[108] BBC Online (2006) Government's control order ‚problem'. Available at http://news.bbc.co.uk/1/hi/uk_politics/5127388.stm . And Times Online (2006) UK terror suspect wins challenge against control order. Available at http://www.timesonline.co.uk/article/0,,200-2130811,00.html .

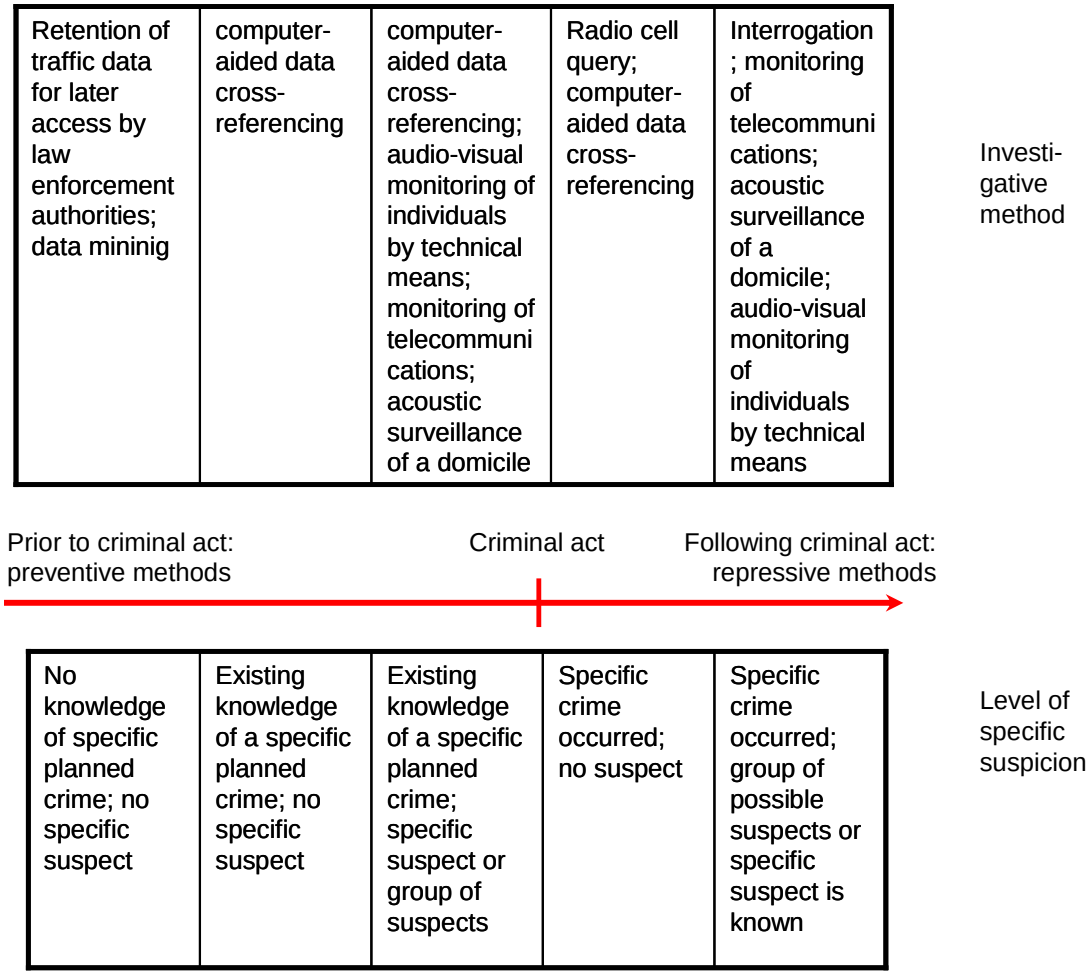

Figure 2: Investigative method and level of suspicion

The less knowledge of specific plans exists, the more individuals are covered by investigative methods as at this point in time the intention is to find 'the needle in the haystack'. In order to detect conspiracies to commit specific criminal acts information from various sources must be aligned and minded for behaviour that is for some specified reason suspicious. Investigations at this stage must carefully consider proportionality of the method chosen as mostly innocent individuals will be subject to the investigation.[109]

[109] See Chapter 4.

Chapter 3 Privacy Impacts of identified Basic Technologies

3.1 The Basic Technologies

In order to categorize general privacy risks and to make an analysis of security technologies easily conferrable PRISE developed a generic model of basic (or underlying) technologies.[110] All security technologies can be mapped to these basic technologies, comprising one or several of the technologies.

PRISE differentiates four basic technologies:

- *Sensor technology:* Sensors produce an output signal of the value of a measured property. It is possible to differentiate electromagnetic, mechanical, thermal, chemical, acoustic, optical and radiation and other types of sensors.

- *Communication technology*: Communication technology performs the transmission of data from source A via step B to end C. In the context of PRISE communication technology covers landline communication like transmission over the fixed telephone network, a database backend-system or a local area network as well as transmission in wireless networks. Any electronic way of transmitting and sharing data is regarded a communication technology.

- *Data Storage*: Data storage is used for the technological means to retain data on a storage medium.

- *Analysis and Decision Making*: Analysis and Decision Making is used for technologies further analyzing collected or stored data by matching it against a reference database or cross-referencing it. Analysis and decision making is used for authentication, profiling and data-mining.

[110] See description in PRISE Deliverable 2.2 Overview of Security Technologies, Chapter 2.

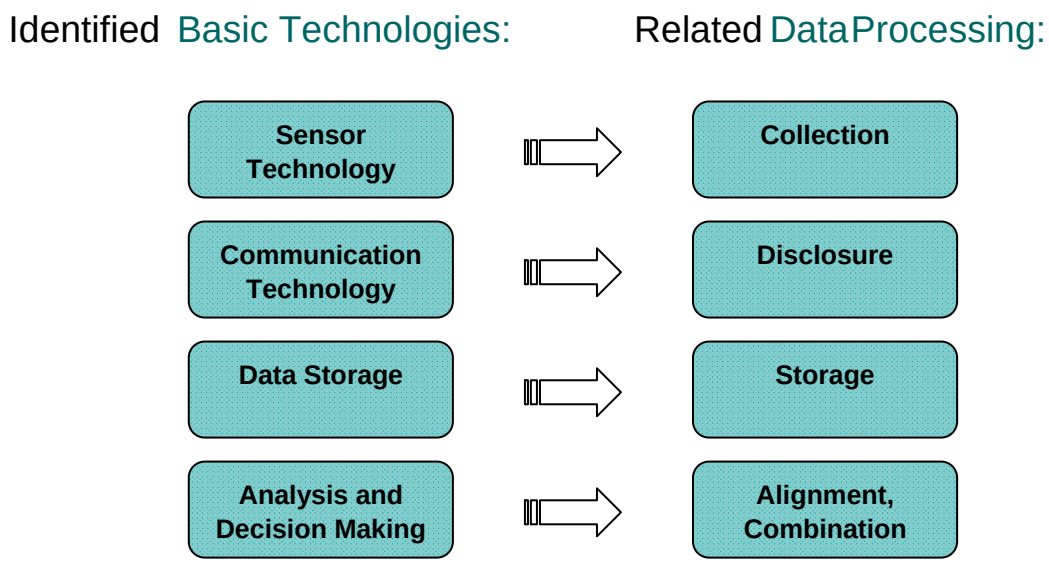

Figure 4: Identified basic technologies and related data processing

The generic approach of this model will be further elaborated here, in order to show its relevance for a systematic approach to a first analysis of existing and also future security technologies.

The basic technologies match legally defined forms of data processing. On a European level this definition is laid down in Article 2 (b) of Directive 1995/46/EC whereby *'processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'*. Every step of processing must comply with the legal requirements for the processing of personal data. Thus, while the collection and storage of data may still be covered by a legal provision, using this data for a new purpose (function creep) possibly will not. While PRISE draws basic privacy principles from the existing international and European regulatory frameworks, a detailed analysis would always have to include the applicable national regulations, too.

The assessment of legal compliance when developing a security technology can be integrated into the research and development process of companies and should be integrated at an early stage in order to already focus on privacy compliance when defining the functionality of the future product. Otherwise, if a compliance assessment is conducted only at the end of the research process, necessary changes will lead to disproportional higher costs as parts of the product might have to be redesigned. A proposal on how to introduce Data Protection

Management into the organisational structure of security research and development will be further described in the PRISE Proposal Report.[111]

3.2 Known Privacy Implications of the Basic Technologies

With regards to specific technical features of the basic technologies, general conclusions on possible privacy implications can be drawn. These inherent implications are likely to exist in security technologies consisting of one or more of the basic technologies. Technical proposals on how to deal with these implications to achieve, where possible, privacy enhancement will be presented in the. Proposal Report.

3.2.1 Sensor Technology

Sensors can come in different sizes. Even with easily visible ones (like CCTV) the data subjects lacks transparency on the fact that data has been collected at all and also which data was collected and possibly transmitted or stored. This lack of transparency is even more intense where the sensor is not visible or otherwise noticeable to the data subject. As indicated above, transparency can not prevail in the cause of a covert investigation.

Some of the measured data may reveal intimate information like race, ethnicity, mood or medical conditions and thus be sensitive data requiring special attention with regards to further processing and legal grounds.

Secondly, many sensors will collect data from any property measured from all objects or persons within the sensor's range, not differentiating between possible suspects and innocent individuals and may therefore violate the proportionality principle.

3.2.2 Communications Technology

Communication technology shows several privacy implications. Communication (or transfer of data) may take place unobserved and thus lack transparency. Communication is vulnerable to different types of attacks such as eavesdropping interception, and unauthorized access. RFID tags for example usually communicate with every reader within range. Protecting the transmission may require authentication, encryption, implementation of an authorisation concept and logging of access.

3.2.3 Storage Technology

The privacy implications with storage are: data security (preventing unauthorized access and loss of data), the question whether the legally required period of retention is technically assured by deletion procedures, the question of verification of correct and lawful collection and access.

[111] PRISE Deliverable 3.3 Proposal Report

Furthermore, the linkability of personal data stored in different databases intensifies the privacy impact for the data subject as through linking data additional information may be attained which could not have been drawn from the separated sources.

3.2.4 Analysis and Decision Making

Analysis and Decision Making procedures will possibly lack any transparency for the data subject as neither notification on which data sources are linked, nor on when the mining procedure takes place is usually given. Depending on how concrete a suspicion of a specific criminal offence planned or committed is, mining huge sets of data from various sources and relating to many data subjects, may lack proportionality.

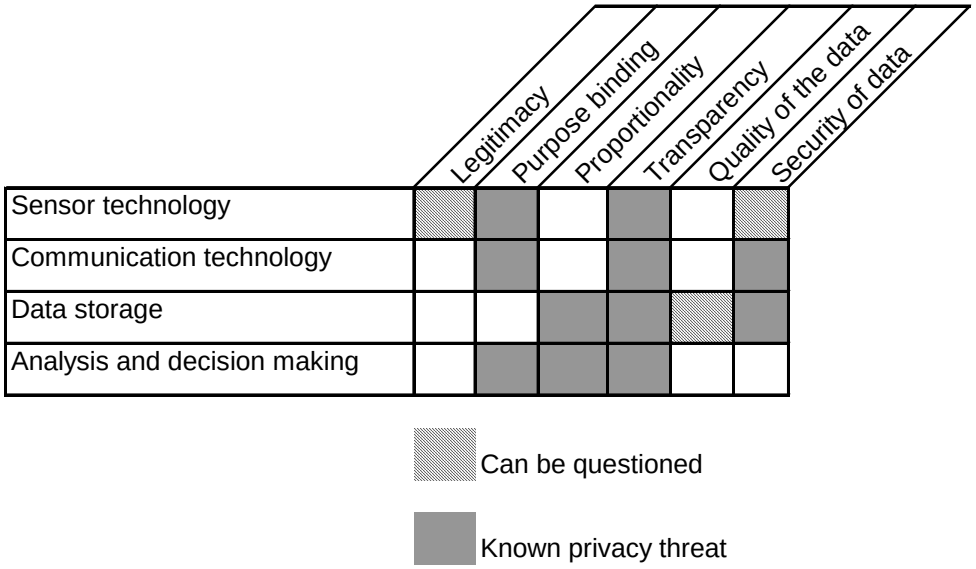

Figure 5: Known Privacy Threats of basic technologies

3.3 Combinations of basic technologies and their consequences

Examples illustrating the impact of a combination[112] of several basic technologies in an application are wireless sensor networks[113]. In some cases, privacy relevance of a technology results only from a combination of several technologies because the information is linked to an individual and combining technologies possibly intensifies this privacy impact, too. Wireless

[112] See also S. Ham and R.D. Atkinson (2002) Using Technology to Detect and Prevent Terrorism, available at http://www.ppionline.org/documents/IT_terrorism.pdf.

[113] See for example USA Today (February 2007) Wireless sensors extend reach of the Internet into the real world, available at http://www.usatoday.com/tech/wireless/data/2007-02-12-wireless-sensors_x.htm.

sensor networks generally consist of a data acquisition network and a data distribution network and can be used for behavioural monitoring.[114] Wireless sensor networks combine multifunctional sensor nodes which include sensing, data processing, and communicating components with wireless communications. The sensors transmit data of the sensed phenomenon to central nodes where computations are carried out and data is fused. Sensor nodes cover self-organizing capabilities and can adjust to changing physical conditions. Such smart environment monitoring technologies lead to an increased level of privacy intrusion, not only because their functionality is lacking transparency. A combination of all basic technologies will increase the complexity of a technology and possibly also combine many of the inherent privacy issues of the basic technologies.

3.4 Conclusion for future technologies

Even yet unknown technologies follow the same approach with respect to data flows and processing. They will collect data, possibly transmit it, store it and further analyse it. Systems will become even smaller, even more complex and may be used even earlier in the investigation process, or even as a means of detecting an intention of foul play. This could include looking for first traces and patterns of suspicious behaviour or to identify individuals or acts meeting the profile of possible terrorists. We envision that new emerging technologies like ubiquitous surveillance technologies will not have new privacy implications as they are going to be based on the here identified four basic technologies. They will however very likely have an intensified impact on privacy as technological possibilities are ever increasing. Technology advances continuously, so it is up to the legislator[115] to put an end to not encourage even more intrusive security technologies in the future by reflecting ethical issues in law.

[114] F.L. Lewis (2004) Wireless Sensor Networks, available at http://arri.uta.edu/acs/networks/WirelessSensorNetChap04.pdf and I.F. Akyildiz et al (2002) Wireless sensor networks: a survey, available at http://www.coe.uncc.edu/~jmconrad/ECGR6185-2005-01/notes/SensorNet02.pdf .

[115] See also S. Ham and R. D. Atkinson (2004) Technological Innovation Without Big Brother – Privacy Principles for Government in the Information Age, available at http://www.ppionline.org/documents/bigbrother_0929.pdf.

Chapter 4 Limits to the restriction of Privacy

In this chapter case law of the ECHR and the German Constitutional Court which examines the relation of investigation methods and their impact on fundamental rights will be presented.

4.1 The debate on a balance between Security and Privacy

Many reports and papers[116] have discussed the dilemma between ensuring inner security and infringement of fundamental rights in the course of doing so. When discussing the relation between inner security and privacy, it is necessary to first define the perspective of whose security shall be safeguarded and how a state of security would look like. Also, in this context it is necessary to further define terrorism and distinguish it from organised crime as the perceived threat of terrorist attacks is taken to justify the extend investigative powers of police and secret service.

The PRISE Criteria Report[117] will further elaborate the societal dimension of this relation. Legal limits are presented subsequently exemplified by case law.

4.2 Case law of the ECHR

The European Court of Human Rights delivers binding judgements[118] on applications from individuals and states alleging violations of the Convention for the Protection of Human Rights and Fundamental Freedoms.

Concerning the question of secret surveillances the ECHR[119] has ruled on several occasions[120] that a lack of an adequate legal basis leads to the finding of a violation in respect of secret surveillance and similar infringements of privacy.

Article 8 of the Convention guarantees the right to respect for private and family life, home and correspondence. The leading case on surveillance is *Klass v. Germany*[121]. The Court ruled that the restriction of free communication constitutes a direct interference with art. 8 and that powers of secret surveillance of citizens were tolerable under the Convention only insofar as strictly necessary for safeguarding democratic institutions. The necessity of some degree of

---

[116] See for example T. Lynch (2002) Breaking the Vicious Circle – Preserving Our Liberties while Fighting Terrorism; D. Haubrich (2003) September 11, Anti-Terror Laws and Civil Liberties: Britain, France and Germany compared; L. Zedner (2005) Securing Liberty in the Face of Terror: Reflections from Criminal Justice; V. Zöller (2005) Liberty dies by Inches: German Counter-Terrorism Measures and Human Rights; K. Waechter (2006) Die Menschenrechte und der Schutz der Inneren Sicherheit im 21. Jahrhundert Neue Tendenzen im Sicherheitsrecht – Spiegel eines sich wandelnden Werte- und Verfassungsverständnisses? (in German); B. Hayes (2006) There is no "balance" between security and civil liberties – just less of each.

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

[118] The obligation to abide by the final judgement of the court is regulated in Article 46 § 1 of the Convention.

[119] See analysis of case law 2005, available at http://www.echr.coe.int/NR/rdonlyres/C8B96BB2-45AF-49DF-9738-75D5117EA5D0/0/2005analysisofcaselaw.pdf.

[120] For example Malone v. the United Kingdom, judgement of 2 August 1984; Halford v. the United Kingdom, judgement of 25 June 1997; Kopp v. Switzerland, judgement of 25 March 1998; Huvig v. France, judgement 0f 24 April 1990; Kruslin v. France, judgement of 24 April 1990; Valenzuela Contreras v. France, judgement of 30 July 1998; Van Rossem v. Belgique, judgement of 9.12.2004; Vetter v. France, judgement of 31. May 2005; Agaoglu v. Turkey, judgement of 6 December 2005.

[121] Klass and Others v. Germany, judgement of 6. September 1978.

surveillance was explicitly accepted by the Court. Yet, surveillance following this ruling is only permissible if the establishment of facts by any other method is without prospects of success or considerably more difficult.

After discontinuation the intercepted person shall be notified unless notification would obstruct the long-term goals of surveillance.

Furthermore, the Court emphasized in *Malone v. United Kingdom* the need for clarity in legislation of surveillance measures.

Conclusions drawn from the ECHR are: Measures restricting rights laid down in art. 8 of the Convention have to be laid down by law, must have a legitimate aim such as national security, be necessary in a democratic society and strictly proportionate. As laid out in *Klass v. Germany*, proportionality is crucially determined by sufficient safeguards to ensure that the measures are not carried out in an excessive or arbitrary manner.

4.3 Case Law of the German Constitutional Court

The German Constitutional Court has for historic reasons a strong position in the German legal system of checks and balances and it exercises the right to void unconstitutional laws very consistently.

The court has ruled on numerous aspects of investigative powers and privacy matters. These cases include:

- Census of population[122],
- Acoustic surveillance of private homes[123],
- Telecommunication interception measures[124],
- Preventive dragnet investigation (computer-aided search)[125],
- Storage of DNA sample for later identification[126].

The court has acknowledged a that core sphere of privacy which must not be infringed even for safeguarding inner security. This core sphere covers intimate and personal conversations and expressions in the suspect's domicile. Evidence (recordings) touching the core sphere must not be collected. If in the cause of an acoustic surveillance of a suspects' home the law enforcement agent carrying out the surveillance realizes that inside the suspects' home

[122] Volkszählungsurteil, BVerfGE 65, 01.
[123] Großer Lauschangriff, BVerfGE 109, 279.
[124] TKÜ, BVerfGE 100, 313.
[125] Präventive Rasterfahndung, BVerfG Beschluss of 4. April 2006.
[126] DNA-Identitätsfeststellungsmuster, BVerG Beschluss of 18. January 2001.

conversations and expressions are touching the core sphere, the surveillance must be stopped immediately.[127]

Furthermore, the Court has ruled that the general threat of possible terrorist attacks is not sufficient to justify computerized screening of databases. Such a screening would only be permissible if a specific threat to significant rights exists.

The court has laid down thresholds for interventions and their impact on privacy (in Germany: the constitutional right of informational self-determination).

Fundamental rights interferences must be proportionate, whereby the proportionality principle in German constitutional law means that

- 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.

The security of a state and an individual are high ranking constitutional values.[128] Measures aiming at enhancing or ensuring security or protecting life, physical integrity or freedom of citizens aim at achieving legitimate purposes.

When balancing the adequacy of an interference with fundamental rights, the intensity of the interference must be assessed. The Constitutional Court has developed a set of criteria which indicate the intensity of a fundamental right interference:

- how many bearers of a fundamental right are affected by the measure at question,
- how intensive is the impact
    - which kind of data is collected; sensitive data[129] or data protected by other constitutional rights like the inviolability of an individuals home or of the mail,
    - does the measure involve data fusion or linking of data,
    - do subjects of the investigative measure remain anonymous,
    - which disadvantage could the measure result in
- which requirements apply to the measure

---

[127] Article 13 of the German Basic Law (the German Constitution) was changed according to the ruling of the Constitutional Court.

[128] BVerfG Beschluss of 4th April 2006.

[129] That is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life, Article 8 of Directive 1995/46/EC.

- has the person given reason to be subject of an investigation or is the investigation carried out without reason

The Constitutional Court does not hold the view that all intensive interferences with fundamental rights like privacy is always unconstitutional. But it regards an intensive interference to be proportional only if a substantial barrier (*Eingriffsschwelle*) for its execution is complied with. This means a sufficiently concrete risk for a high ranking constitutional value must exist for an intensive interference to be proportional.

This consistent position of the Constitutional Court clearly indicates that it applies strict requirements to the proportionality of investigative measures which result in privacy interference. A state of zero privacy is not covered by German constitutional law even in the context of criminal investigations and application of security technologies.

The court's findings are based only on principles which can also be considered basic findings of the above described case law of the ECHR. It further elaborates criteria for the strict proportionality of measures restricting privacy.

The proportionality principle is an irrevocable basis of state measures. The requirements of the German Constitutional Court are presented here because conclusions on technical design of security technologies can be drawn from them[130] and because they are a consistent means to assess the proportionality of privacy infringing investigative measures.

4.4 Conclusion

The presented case law indicates that there is no state of zero privacy even in the context of safeguarding inner security. The developers of technologies, the legislator of investigative powers as well as law enforcement authorities using a technology in a specific investigation have to comply with the proportionality principle and must not use excessive means. The less concrete a suspicion or knowledge of a planned criminal offence the more attention has to be given to the relation of the foreseeable efficiency of the planned investigation, the number of affected individuals and the intensity of intrusion conveyed by the specific investigation method. Possible questions that could be raised to define the intensity of intrusion are: Is the investigation covert? Does it take place in a domicile? What is the duration of the investigation? Are sensitive data processed?.

[130] See D 3.3 Proposal Report.

References

- Books
  - EPIC and Privacy International (2005) Privacy & Human Rights 2005: An International Survey of Privacy Laws and Developments. Available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-542783 .

- Journal Articles
  - Agrawal, D. and Aggarwal, C. (2001) On the Design and Quantification or Privacy Preserving Data Mining Algorithms, available http://citeseer.ist.psu.edu/cache/papers/cs/25580/http:zSzzSzweb.mit.eduzSzcharuzSzwwwzSzprivate.pdf/agrawal01design.pdf.
  - Akyildiz, I.F. et al (2002) Wireless sensor networks: a survey, available at http://www.coe.uncc.edu/~jmconrad/ECGR6185-2005-01/notes/SensorNet02.pdf
  - Foundation for Information Policy Research FIPR (2003) Communications surveillance briefing, available at http://www.fipr.org/030818ripa.html.
  - Ham, S. and Atkinson, R. D. (2002) Using Technology to Detect and Prevent Terrorism. *Progressive Policy Institute Policy Brief*, January 2002. Available at http://www.ppionline.org/documents/IT_terrorism.pdf.
  - Ham, S. and Atkinson, R.D. (2004) Technological Innovation Without Big Brother – Privacy Principles for Government in the Information Age, available at http://www.ppionline.org/documents/bigbrother_0929.pdf.
  - Haubrich, D. (2003) September 11, Anti-Terror Laws and Civil Liberties: Britain, France and Germany compared.
  - Hayes, B. (2006) There is no “balance” between security and civil liberties – just less of each.
  - Lewis, F.L. (2004) Wireless Sensor Networks, available at http://arri.uta.edu/acs/networks/WirelessSensorNetChap04.pdf.
  - Liu, K. (2006) Privacy Preserving Data Mining Bibliography, available at http://www.csee.umbc.edu/~kunliu1/research/privacy_review.html.
  - Lynch, T. (2002) Breaking the Vicious Circle – Preserving Our Liberties while Fighting Terrorism

- Norris, C. (2006) A Report on the Surveillance Society: Criminal Justice, available http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_appendices_06.pdf.

- Oosting, D. (2006) Europe's clampdown on terrorism risks backfiring. *Europe's World*, Spring 2006, pp. 131 – 137.

- Sweeney, L. (2002) *k*-Anonymity: a model for protecting privacy, available at http://privacy.cs.cmu.edu/dataprivacy/projects/kanonymity/index.html.

- The Surveillance Studies Network (2006) 'A Surveillance Society' at http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_report.aspx.

- Waechter, K. (2006) Die Menschenrechte und der Schutz der Inneren Sicherheit im 21. Jahrhundert Neue Tendenzen im Sicherheitsrecht – Spiegel eines sich wandelnden Werte- und Verfassungsverständnisses?.

- Zedner, L. (2005) Securing Liberty in the Face of Terror: Reflections from Criminal Justice.

- Zöller, V. (2005) Liberty dies by Inches: German Counter-Terrorism Measures and Human Rights.

- Government Publications

  - Wiesner, Jerome. B (1971) *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the House Committee on the Judiciary*, 93d Congress, 1st Session Part I, 761-774.

  - Council of Europe Committee of Experts on Terrorism (CODEXTER) (2005) *Profiles on Counter-Terrorism Capacity Austria*. Available at http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Fight_against_terrorism/4_Theme_Files/Country_Profiles/ .

  - Council of Europe Committee of Experts on Terrorism (CODEXTER) (2006) *Profiles on Counter-Terrorism Capacity Spain*.

  - The Home Office on the national DNA database at http://www.homeoffice.gov.uk/science-research/using-science/dna-database/.

  - Parliamentary Office of Science and Technology (2006) Postnote – The national DNA database, available at http://www.parliament.uk/documents/upload/postpn258.pdf.

- Newspaper Articles

  - BBC Online (2006) Government's control order ‚problem', available at http://news.bbc.co.uk/1/hi/uk_politics/5127388.stm.
  - BBC (January 2006) Juveniles' DNA recording defended, available at http://news.bbc.co.uk/1/hi/uk/4633918.stm.
  - BBC (June 2006) DNA database is shared overseas, available at http://news.bbc.co.uk/1/hi/uk_politics/5056450.stm.
  - International Herald Tribune (January 2007) Constitution and trade at top of Merkel's EU agenda, available at http://www.iht.com/articles/2007/01/17/news/europe.php.
  - International Harald Tribune (January 2007) Germany seeks to modernize policing across Europe, available at http://www.iht.com/articles/2007/01/15/news/germany.php.
  - The Guardian (July 2002) Blunkett security laws may be illegal available at http://politics.guardian.co.uk/homeaffairs/story/0,11026,766563,00.html.
  - The Register (November 2006) Number plate cameras could be illegal, says surveillance commissioner, at http://www.theregister.co.uk/2006/11/30/anpr_legality_debate/.
  - The Telegraph (October 2006) DNA database 'should include all', available at http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/10/24/ndna24.xml.
  - Times Online (2006) UK terror suspect wins challenge against control order. Available at http://www.timesonline.co.uk/article/0,,200-2130811,00.html.
  - USA Today (February 2007) Wireless sensors extend reach of the Internet into the real world, available at http://www.usatoday.com/tech/wireless/data/2007-02-12-wireless-sensors_x.htm.

Table of figures