PRISE
privacy security

Security Research

PASR

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

Workshop Paper

PRISE

User and Stakeholder workshop II

Vienna

4 February 2008

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

Legal notice:
The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of the following information.

Table of Contents page

Table of Figures

User and Stakeholder Workshop Vienna - Programme

Guidelines and Criteria for Privacy Enhancing Security Technologies
Second PRISE User and Stakeholder Workshop

4th of February 2008

10:00 – 18:00

Austrian Academy of Sciences

Dr. Ignaz Seipel-Platz 2, Vienna,

Austria

The PRISE consortium organises two user and stakeholder workshops, where mid-term results are discussed with stakeholders and policy-makers. The first workshop discussed the results created in the first project phase. The second workshop in February 2008 will focus on the outcomes of the participatory Technology Assessments and of the improvement of the draft criteria for privacy enhancing security technologies.

To a large extent the participants are the same in both workshops, serving as a kind of extended reference group. The invited participants represent suppliers of security technologies, law enforcement, policy shaping, implementers, users, suppliers of data, data protection authorities and NGOs representing human rights concerns.

Please consult the PRISE website http://prise.oeaw.ac.at/ for more information on the PRISE-project, its current results and the workshops.

Knowledge created in the second phase of the project will provide a starting point for the discussions at this second User & Stakeholder workshop. Central topics will be:

- Privacy enhancing design of security technologies – a feasible call?
- How to improve the content of the criteria matrix?
- How can we assess and balance security gain?
- The matrix and the public opinion? – Participatory citizen involvement
- Data protection management process for R&D and security technology users
- How to put the matrix at use

Preliminary Programme

09:30 – 10:00 Registration, Coffee

Plenary:

10:00 – 10:30 ***Welcome and introduction***, Johann Čas, Institute of Technology Assessment, Austrian Academy of Sciences

Short presentation of the participants

10:30 – 11:00 ***Presentation of the Framework – the PRISE Matrix,*** Walter Peissl, Institute of Technology Assessment, Austrian Academy of Sciences and Maren Raguse, Independent Centre for Privacy Protection Schleswig-Holstein (ICPP), Germany

11:00 – 12:30 ***Keynotes and open discussion***
Gus Hosein, London School of Economics and Political Science, UK
Thomas Petri, Deputy Commissioner for data protection and freedom of information, Berlin, DE

12:30 – 13:30 Lunch

13:30 – 14:00 ***Presentation of the results of the pTA activities*** – Interview Meetings on Privacy and Security in 6 countries, Anders Jacobi, The Danish Board of Technology

14:00 – 14:15 ***Presentation of Test Case,*** Christine Hafskjold, The Norwegian Board of Technology

In groups:

14:15 – 15:00 ***Group work*****:** Test of Criteria

15:00 – 16:00 ***Parallel workshops*** *on the basis of the framework presentation, criteria test experiences and citizen consultation*

- How to improve the content of the criteria matrix?
  Facilitator / rapporteur: Maren Raguse
- How can we assess and balance security gain?
  Facilitator / rapporteur: Walter Peissl
- The matrix and the public opinion?
  Facilitator / rapporteur: Anders Jacobi
- How can the matrix be put to practical use?
  Facilitator / rapporteur: Johann Čas

16:00 – 16:15 Coffee Break

Plenary:

16:15 – 17:00 ***What we learned from the workshops*** – how to improve the criteria?
Reports by the rapporteurs and open discussion

17:00 – 17:15 ***Conclusions from the day***, Lars Klüver, The Danish Board of Technology

17:15 – Farewell drinks

20:00 – Dinner at **Schöne Perle**, 1020 Wien, Große Pfarrgasse 2, www.schoene-perle.at

Practical information

PRISE - Workshop:
Guidelines and Criteria for Privacy Enhancing Security Technologies

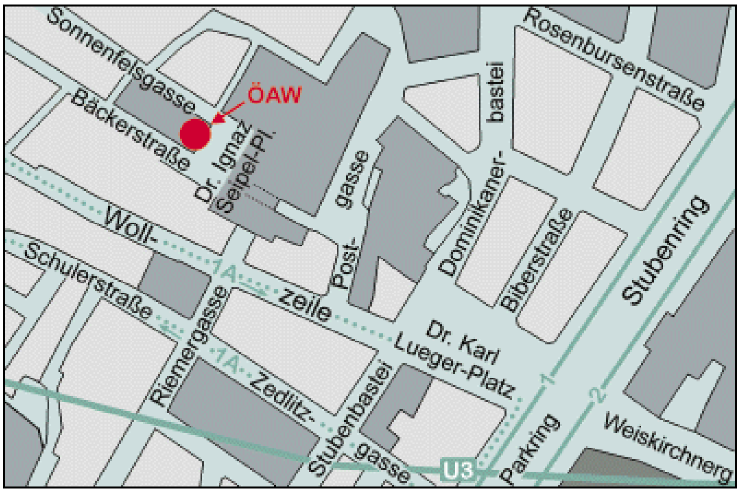
Monday 4 February 2008, 10:00 – 18:00

The conference venue

Austrian Academy of Scienes
Dr. Ignaz Seipel-Platz 2
1010 Vienna, Austria
Tel.: (+ 43 1) 51581-0 / (+ 43 1) 51581- 6582
Fax: (+43 1) 710 98 83
E-mail: prise@oeaw.ac.at

The 2nd User and Stakeholder Workshop of PRISE takes place in the city centre of Vienna, at the premises of the Austrian Academy of Sciences, Dr. Ignaz Seipel-Platz 2.

The next underground station: U3, Stubentor, exit Wollzeile



Transport and Accommodation

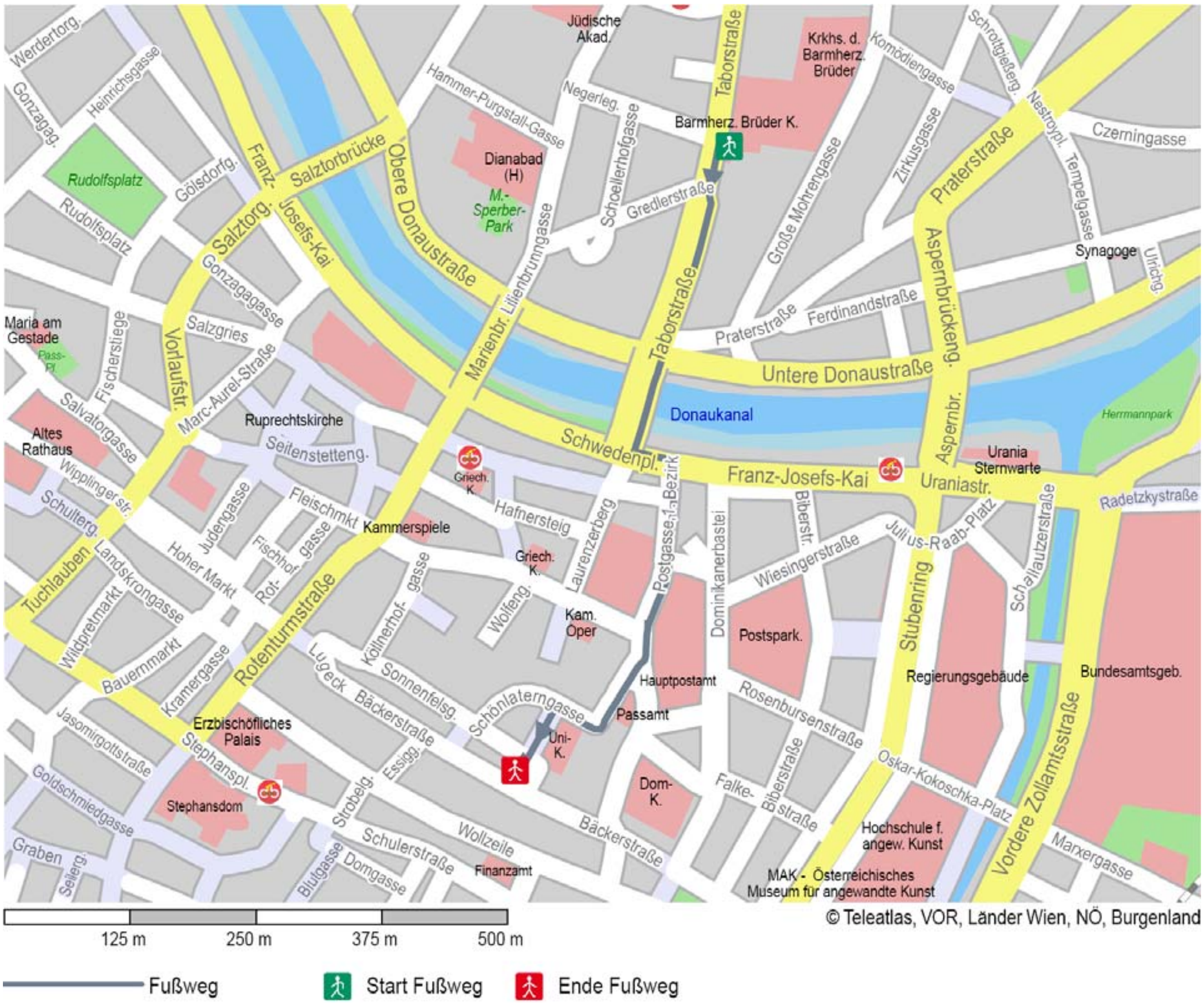
Accommodation and travel expenses can be covered by the project budget. At the PRISE website you can find more information on the recommended Hotel Stefanie and the form needed for reimbursement: http://prise.oeaw.ac.at/workshops.htm

Airfares can be reimbursed on the basis of the economy class tickets available at the time of the invitation, allowing for travel on weekdays. We kindly ask you to enclose a copy of the air ticket and the original boarding passes when sending us your expense sheet.

For more practical information please contact **Sabine Stemberger**, Institute of Technology Assessment, Austrian Academy of Sciences, mail: sabine.stemberger@oeaw.ac.at , Tel.: +43 1 51581 6586.

Find your way from Hotel Stefanie to the Workshop venue

The recommended Hotel Stefanie is located at Taborstraße 12. Next station is U1 and U4 Schwedenplatz. Walking distance to the workshop venue at Dr. Ignaz Seipel-Platz is app. 800 meters/10 minutes.



© Teleatlas, VOR, Länder Wien, NÖ, Burgenland

PRISE work of the second project phase – introduction to the workshops

The following chapters present an overview on the work of PRISE in the second working period. We will provide a summary of the outcome of the participatory events conducted in 6 European countries. And we will introduce the PRISE matrix as the framework for our work of defining criteria for privacy compliant and privacy enhancing security technologies.

The second user and stakeholder workshop is designed to give room to discussions in small working groups, which are devoted to specific themes:

Workshop 1: The matrix and the public opinion.

Workshop 2: How can we assess and balance security gain?

Workshop 3: How can we improve the content of the criteria matrix?

Workshop 4: How can the matrix be put to practical use?

At first we give a short description of the developed framework for criteria development– the PRISE matrix. This is the core model of the project and is needed in all workshops.

The subsequent chapters are structured according to the workshop themes:

Workshop 1 will deal with the results of the participatory activities conducted in six European countries and their incorporation into the matrix and into the criteria – the overall outcome of PRISE.

Workshop 2 will deal with different approaches to security and especially with the question of how to assess security gains. This seems to be necessary to bring the supposed security gain of security technologies into the core discussion of proportionality.

Workshop 3 will have a close look at the PRISE matrix and will generate feedback how to improve it. This workshop will discuss the core procedures behind the PRISE matrix.

Workshop 4 will discuss ways to support the widespread use and diffusion of the PRISE matrix and the developed forms. It will deal with their practicability for proposal writers and evaluators as well as with required adaptations to fit a broader range of potential users.

The PRISE Approach – criteria for privacy enhancing security technologies

Proposals submitted in response to FP 7 call for tenders have to meet high ethical standards as explicitly stated[1] by the European Commission. In the context of security technologies the core of an evaluation should certainly focus on the privacy compliance of planned research. But even if a proposal may include feasible considerations and precautions regarding privacy impact and compliance, it may still not be recommended for funding according to the criteria developed by PRISE if the proposal fails to plausibly show a positive impact on security for European citizens and European states. In addition to an evaluation of product- and process-related privacy criteria it is also necessary to consider the technology's impact on security and the trade-off between privacy and security fostered by the technology.

PRISE aims at developing criteria, which are applicable on different levels (research, development, procurement, implementation) and by different actors (research coordinators, industry, policy makers, public and private users). The main focus at this stage is on the applicability of the PRISE model within the framework of FP7 proposal writing and evaluation. Therefore in D6.1 'Draft Criteria for privacy enhancing security technologies', after the theoretical discussion of the security discourse in the EU, we present a methodology of deducing the criteria and end up with two very short checklist-like forms for proposal writers in R&D as well as for evaluators of these proposals. These two forms are supplemented by a ”textbook”, providing explanations and recommendations on tools, and on how to fulfil the requirements of the included criteria.

The basic idea of the PRISE model is a three-step approach to privacy enhancing technologies. First of all new security technologies have to comply with a minimum baseline. That means there is a core-sphere of privacy that never should be intruded. Second, new security technologies should comply with existing privacy laws, and furthermore as a third step they should be designed according to principles of privacy enhancing technologies (PETs) – the step further.

The presented PRISE approach is based on a set of questions providing guidance for writing and evaluation of research projects; The questions are complemented by detailed discussions of the underlying considerations. The PRISE-matrix below presents the basic framework – the outline of the matrix with the questions filled in. To improve readability and due to limited space the other fields of the matrix are not filled in. For details readers will be referred to the handbook, which is part of D6.1.

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

The PRISE-Matrix[2]

The matrix

The PRISE criteria matrix serves two purposes. It aims to ensure that all aspects relevant for an assessment of a security technology’s privacy impact are taken into consideration. The matrix is directed at research and development (R&D) entities and consortia preparing proposals within the security research theme of FP7 and FP7 evaluators commissioned to evaluate those proposals. The matrix is aimed to serve as a guideline for them, again ensuring all relevant aspects are considered. In case the proposal does not address them even though this appears necessary, the matrix points to lacking discussions of the identified issues.

The matrix differentiates three levels of analysis. A first step – the minimum or ‘baseline’ requirement of privacy protection – aims at assessing whether the technologies allows for the collection or processing of intimate data[3] (data about sex life, sexual preferences, intimate thoughts and conversations, conversations with oneself). Processing and collecting intimate data must be avoided in the first place (data minimization) as it significantly increases the possibility of lacking proportionality and legitimacy. Taking Germany as example, collecting and processing intimate data has been ruled unconstitutional by the German Constitutional Court. Whether a technology’s features and data processing is relevant in this context is enquired by questions presented in the ‘Criteria/Questions’ column of the matrix.

If relevance is identified, the matrix subsequently (in the next column) presents references to tools described in the textbook. These are tools available to encounter the privacy relevant feature. Not all possible tools for achieving privacy compliance are merely technical measures. In fact, technical measures which ensure compliance with all privacy principles identified[4] in deliverable D3.2 ‘Legal Report’ does not always exist. Compliance requires consideration of organisational measures to be implemented by the later user of the product. As an example, technical enforcement of legitimacy and proportionality are hardly thinkable. Ensuring the technology is used in a least infringing way, thus serving as the least intrusive means to achieve the legitimate purpose, requires weighing the underlying investigation and the specific rights and obligations assigned to the data subject as well as the law enforcement or other public authority using the technology. This assessment cannot be mapped technically or designed into the technology as an automated function. The user must carry out this assessment during every investigation and prior to each technology use on a case-by-case basis.

Consequently, PRISE takes a broader approach and in addition to technical tools also discusses organisational tools backing and supporting technical measures, as well as legal tools, which are not in the hand of the R&D company or consortium. The tools referred to in the matrix are elaborated on in the handbook.

In the case of security technologies allowing for the collection of intimate data, no technical tools enabling compliance of this feature are presented as a core sphere of individual privacy represents the limit of privacy, which even for the purpose of safeguarding security must not be infringed. However, the research consortium should assist the later user of its technology by implanting features enabling the user to meet his legal duties such as meeting data subjects’ information rights.

[2] For an in-depth description please refer to the handbook as part of D6.1.

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

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

The finding whether tools exist to enable compliance in case of an identified privacy risk results in a warning in the next column. If tools are available to achieve compliance and the consortium plans to implement them a green light is suitable. Otherwise, a red light would be issued.

Questions ensuring the consortium will consider all relevant aspects of their research and its privacy impact comprise – broken down to the three described levels. The following figure presents the PRISE matrix:

	Criteria	**Tools**			**Warning Interim Status**	**Recommendations for…**		**Conclusions**
	Questions	**Legal**	**Organisational**	**Technical**	**Red/ Green Light**	**R&D**	**Users**	
Baseline	Does the proposal allow / aim at surveillance in homes? Does the proposed technology allow / aim at collection or processing of intimate data? Does the proposed technology allow or aim at interaction with partners like spouse, children, lawyer, priest?							
Data protection compliance	Does the technology lack a specification of the purpose of use and data collection or is the purpose given very broad? Does possible technology use and data collection and processing require passing a new legal basis? Is there a less intrusive means available allowing to achieve the intended result with comparable efficiency? Does the technology aim at or allow the collection of sensitive data? (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction) Does the technology involve linking of data, data fusion or data analysis? Does the technology require lifting anonymity of data subjects? Is the technology used regardless of whether the individual is suspected of any wrongdoing? Is lack of transparency regarding technology use (prior to and/or after use) the default setting?							
Context sensitive trade-off	Does the proposed technology interfere with human dignity? Does the proposed technology interfere with physical integrity of people? Does the proposed technology aggravate judicial scrutiny? Does the proposed technology facilitate societal security? Does the proposed technology aim at crime prevention? Does the proposed technology aim at prosecution? Is the main field of application fight against.. terrorism organized crime random crime Does the proposed technology increase individual security against the state (in terms of privacy protection) in other spheres (economic, social)?							

Figure 1: The PRISE Model for privacy enhancing security technology assessment

Participatory technology assessment – the citizens' views

(Input for Workshop1)

Between May 30th and June 15th 2007, six so-called 'interview meetings' were carried out in Austria, Denmark, Germany, Hungary, Norway, and Spain. The interview meetings combined debate, completing a questionnaire and group discussions. The interview meetings of the PRISE project involved altogether 180 citizens in the six countries. The project resulted in six national reports, and a synthesis report collecting and analyzing the results of the national reports.

The interview meeting

The interview meeting is a method to gain knowledge of what a group of people think and feel about complex technologies. It is not a method that claims to represent the whole population; nevertheless it aims at including a diverse selection of citizens selected on the basis of demographic criteria such as age, gender, education and occupation.

Using group interviews and a questionnaire, a group of about 30 people are asked at the interview meeting about their perceptions and preferences in relation to a technology, a technological development, challenge or problem. As a rule, interviewees do not possess any expert or professional knowledge about the technology in question. However, prior to and during the meeting, the participants are informed of the advantages and disadvantages of the technology in order to give them a balanced and factual common starting point. In the PRISE project, this information is based on the scenarios developed in WP4 and the dilemmas these scenarios focus on.

The two methods of questionnaire and group interviews complement one another well; the questionnaire ensures that all the participants are heard and that there is comparable data relating to the most important areas. The group interview, on the other hand, creates a lively debate and ensures that the participants can include aspects that are not addressed by the questionnaire and that different arguments are articulated.

Results of the Interview meetings

These results of the participatory technology assessment (pTA) activities are a number of important issues that where discussed among the participants across the six countries. These lead to some basic conclusions of attitudes and opinions that are supported by the *vast majority* of the participants. A *vast majority* entails that 80 percent or more of the participants in the six countries have backed these conclusions in the relevant questions in the questionnaire. And finally there are some democratic demands that the participants have emphasised.

Nuanced opinions among participants

The participants at the six interview meetings in the six different countries had a broad variety of opinions and some very nuanced attitudes towards privacy and security. The participants showed great insight as well as willingness to discuss and argue for their opinions and to listen to and learn from the opinion of others. The participants could roughly be divided into three groups; the biggest group is the participants who place privacy over security, the second group is the participants that emphasise the need for security technologies and finally there is a group of undecided participants.

Acceptability of technologies depended on many factors

The participants are very split when it comes to the questions of the necessity of security technologies, the extent of the threat from terror and crime and the balance between privacy and security. Generally, the vast majority feels uncomfortable about their privacy being infringed and can only accept infringement in certain places and situations. Places or situations where the participants find the risk of terror or crime to be increased make the implementation of different security technologies more acceptable to participants. Airports or places with high crime rates are good examples of this. Other factors that make privacy infringing security technologies more acceptable include increased convenience and authorization by court order.

Concerns about new security technologies

The participants have a number of concerns about implementing new security technologies. The concerns are about the technology that is ineffective and that criminals, commercial interest and governmental institutions will misuse it. Some are also concerned about the individuals behind the technology and the amount of personally identifiable information these people can access. The participants also make the point that once technologies are implemented it is unlikely that they will be withdrawn again – even if they prove to be ineffective.

It is interesting to note that the threat of terror does not seem to be as important to the participants as the threat from crime. Furthermore, it is worth noticing that there is a clear limit when it comes to surveillance of the physical body. The participants also indicate that function creep – technologies or data being used for something else than the original purpose – is unacceptable.

Public debate needed

The vast majority of the participants emphasises the need for public debate on questions about implementing new security technologies. They find it very important that new security technology is subjected to sincere evaluation in an open and transparent process that also includes human rights organisations and technology experts before it is implemented. Citizens, experts and human rights organisations must be involved to some degree all the way from research to implementation.

Basic conclusions

The analysis can be summed up in certain basic conclusions based on the input from the vast majority (more than 80 percent) of the participants:

Basic limits of acceptability

- The threat of terror as such does not justify privacy infringements
- Physically intimate technologies are unacceptable
- Misuse of technology must be prevented
- Function creep is not acceptable

What makes security technologies more acceptable?

- Proportionality between security gain and privacy loss
- Court order
- Strict control
- Privacy infringing security technologies must be the last option

Democratic demands

- Public debate
- Broad involvement
- Always analyse privacy impact

Questions to be addressed in workshop 1:

- What impact should the results of Interview Meetings have on the criteria matrix?
- How well is citizens input represented in the criteria matrix now?
- What amendments (if any) would you propose?

Security, security gain and how to assess?

(Input for Workshop 2)

Definitions and concepts

In the context of the PRISE project we defined security as the absence of danger – that is a state where the desired status quo is not threatened or disrupted in any way. Furthermore in PRISE security is understood as the security of the society – or more precisely – of the citizens that constitute the society. (PRISE 2006)[5] Integral part of the PRISE scope is the privacy impact of security technologies. So PRISE is mostly dealing in the area of "inner security" and potential threats to privacy.

Different approaches of security can be found in academic as well as political debates. The state centred traditional approach is nowadays challenged by the Human Security approach. The following table gives an overview on different approaches to security:

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

Table 1: Traditional and human security (Owen 2004, p.17)

In accordance with the scope of PRISE we deal with development and implementation of security measures within Europe, with a global technology transfer perspective. The European Security Strategy as well as the Human Security Doctrine for Europe states the necessity of intervening outside the EU to protect the security of EU citizens. PRISE aims at giving advice to decision makers in the research funding process and in R&D of security technologies to design security technologies in line with fundamental rights. These are the same all over the world. Although PRISE does not primarily assess technologies that are applied in civil and/or (semi-)military use outside the EU its findings may be applied elsewhere too.

To be acknowledged as responsible actor the European Union is supposed to show that human rights are fulfilled within the EU itself. Therefore a thorough discussion has to be undertaken on whether specific measures of security policy are really raising the level of human security internally the EU. Democratic principles like the fundamental rights of privacy or freedom of speech or the freedom of assembly, the division of power between legislation, executive and juridical powers need to be protected. Lowering the barriers may end up in non-democratic societies with no more security.

Dimensions of security

Balancing privacy and security is a challenging task. You should act least intrusive and provide a high level of security. However, the level of security is not easy to measure. It strongly depends on normative orientations and values involved. So there will hardly be any generic security concept. To deal with the problem leads directly to the core concept of proportionality of measures. This proportionality may on

[5] D 2.2 Overview of security technologies

the one hand be reached by doing minimum harm to fundamental rights but on the other hand a higher level of intrusion may be acceptable if the security gain is correspondingly higher. So the assessment of the potential security gains by using a specific technology is a prerequisite to a holistic proportionality assessment.

PRISE tries to deal with a potential security gain from security technologies. In order to be able to do a Security Gain Assessment we differentiate different dimensions of security.

Security of what? In recent security policy discourse main perceived threats are terrorism, organised crime and random crime. In order to assess security gain by using specific security technologies one has to figure out to what extent the respective technologies or measures help to solve problems in the above mentioned areas.

Security for whom? In the PRISE project we will focus on security of individuals within a society. We will not look at national (state) security with its foreign policy and military approach. Security of the individual may be security of intrusion into fundamental rights by public authorities or private entities. By assessing the potential security gain it will be necessary to show how a respective technology has built-in barriers against misuse by end-users, be it public authorities, private enterprises or criminals.

Relationship of security in terms of prevention and prosecution: For assessing a potential security gain it makes a difference whether a technology is used for preventive measures or for prosecution of suspects after a committed crime or terror-attack.

Can security be measured?

There are two different “securities” – and both are socially constructed[6] The “objective security of a society” (if there is such a thing as “objective security”) can easily be assessed by reading statistics on committed crimes and terror attacks. How effective the respective policy was can be seen from statistics over time. Based on this it does not seem to be possible to draw causality to a specific technology and its implementation.

The “second security” is ”subjective security”, which is based on the subjective feeling of security and therefore very difficult to determine. It is however possible to get a glance of what people think by surveys and similar tools. At the same time it seems to be rather clear that socially constructed feelings on insecurity, which are shaped by a multiplicity of parameters cannot easily be re-shaped by monocausal technological approaches. The question remains: How can technology influence the discourse on perceived security?

A methodological problem arises with regard to the measurement of security: How can we measure the non-occurrence of an event? How many acts of terror have been prevented since 2001? How many could have been prevented by traditional means or technologies?

As far as security technology is concerned it seems to be possible to measure the empirical evidence of (increased) security (objective and subjective). One problem remains: it is only possible ex-post. For ex-ante assessment of a potential security gain one will be restricted to a plausibility check of the line of argumentation, one has to look for best practice examples and try to assess the effectivity of the measure (technical/organisational). A possible scale could be: Insufficient, sufficient, or optimized. However, it is a static approach and must be done periodically, because risks and their assessments change over time.

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

Questions to be addressed in workshop 2:

- What kind of security do we need?
- What part does technology play in the security discourse?
- How can security be measured?
- How can security gain be incorporated in proportionality considerations?

PRISE criteria matrix

(Input for Workshop 3)

The objective of workshop 3 is to discuss the current draft approach of the PRISE criteria matrix as presented above (page 11).

The matrix as the core outcome of PRISE is arranged in three steps, (baseline, data protection compliance, context sensitive trade-off) each of which should be considered by the consortium applying for funding as well as the evaluator assessing the proposal. The proposal must indicate which kind of data is going to be collected and processed with the new security technology. If it allows for the collection of intimate data, the technology will face significant problems, at least in Germany[7]. In other member states, proportionality of the use of a technology allowing collection of intimate data is difficult for the users to conduct. If the technology allows for the collection and processing of intimate data, the proposal should discuss which safeguards are implemented to assure this kind of data is not collected and processed.

As a second step the proposal writer should discuss how and if the general concept of the new technology as well as specific features may infringe the privacy principles. The PRISE matrix remains rather abstract on the 'question level' of step 2 (data protection compliance) in order for the matrix to remain usable. Proposal writers can turn to the PRISE handbook for a more explanation and a detailed overview of existing tools to foster legal compliance.

Finally, the proposal needs to address the societal impact and aspects of the research applying for funding. New refined and more efficient security technologies may introduce new technical features, which can reduce or increase the technology's impact on privacy as well as on security. As security solutions exist for many law enforcement authorities' investigational powers the proposal will have to indicate not only how it differs from existing security technologies. A discussion of how the security technology aims to foster security[8] and how the expected security gain relates to the identified privacy risk is required. As the matrix will point the FP7 evaluator to open issues, a lacking discussion in the proposal may have negative consequences for the evaluation of the proposal.

For each of the three levels proposal writers and evaluators can turn to the PRISE handbook listing available tools addressing the identified privacy issues.

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

The evaluator of the proposal will be able to systematically assess whether the proposal touches arising privacy issues of the intended research and discusses tools to heal or reduce privacy implications. The Evaluator's privacy check table suggests assigning red or green lights depending on whether a tool was identified to address privacy issues or not.

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

[8] See D6.1 Chapter 2 for description of different concepts of 'security'.

It is not up the PRISE project to present recommendations regarding a certain number of red lights which ought to lead to rejecting a proposal as this decision must be based on the overall impression of the proposal. An assessment will take into account the characteristics of each proposal and a standardized weighing of the results seems inappropriate. The aim of the PRISE approach is to enable proposal writers as well as proposal evaluators to take a systematic approach regarding privacy implications. The PRISE approach shall support a comprehensive analysis and ensure both parties involved in the application process consider all relevant aspects.

Questions to be addressed in workshop 3:

- Do the three identified levels and subsequent questions enable proposal writers and evaluators to identify all possible privacy issues?

- Which tools (technical, organisational, legal) are available to foster privacy compliance of security technologies?

How can the matrix be put to practical use?

(Input for Workshop 4)

The main objective of this workshop group is to identify, discuss and elaborate measures to increase the practical application of the criteria developed by the PRISE project; both within the context of the 7th Framework Programme Security Research and the widespread debate on security and human rights in general.

This task consists of at least three dimensions. A primary aim of the PRISE project is, on the one hand, to assist proposal writers in taking into account privacy enhancing design principles when developing R&D projects and, on the other hand, to provide a tool for evaluators which allows them to assess to which extent individual proposals are compliant with these principles. The availability of such a tool alone, however, does not guarantee that it is also widely used. Hence the first question to discuss is how to promote the integration of the PRISE criteria into the standard evaluation procedures (within the Security research focus) of the 7th Framework programme and within further national and international security research programmes. Being a part of the regular proposal evaluation will certainly serve as an important leverage for widespread application in security industry and R&D.

Privacy by design, beginning in the R&D phase is certainly a core element of security technologies in line with the human right of privacy. In many practical cases of implementations and applications of information technologies, specifically in the context of inner security, this feature may not be sufficient to ensure the privacy compliant use of a particular technology. Although from an ideal perspective “privacy by design” should disallow any privacy infringing use of a particular product or service, it may turn out that only privacy enabling features can be guaranteed, meaning that the application of the criteria for privacy enhancing security technologies may only be sufficient to constitute the possibility of privacy compliant use in a real perspective. For an actual privacy enhancing impact several further conditions need to be fulfilled: e.g. a preference for privacy enhancing security technologies in the procurement process or the establishment of regulations which support or enforce privacy compliant use. Hence the second aspect is to discuss which other stakeholder- and interest-groups fulfil both conditions: They play an influencing role in shaping the development and use of security technologies and could benefit from the criteria and guidelines provided by PRISE.

Whereas the criteria are based on established sets of generic principles of protection of human rights and privacy, they are presented in a way specific to evaluation procedures applied in EU Framework Programmes. The third central question to discuss is therefore the need of adaptations and adjustments required to be useful also to the broader community of stakeholders and decision makers identified in the previous task. One sub dimension of this discussion could be to identify subsets of criteria relevant for particular groups. This discussion could also include the need of extensions that could possibly be required for a wider application; thus identifying the need for further research beyond the scope of the PRISE project. Another sub dimension to be addressed is the form of presentation to serve the specific needs and expectations of relevant stakeholders and ways to promote dissemination to these groups.

Questions to be addressed in workshop 4:

- How to promote and support the widespread use of the criteria for privacy enhancing security technologies in the preparation and evaluation of R&D in security technologies?

- Which other stakeholders and decision makers should be addressed to increase real world impact of the project results?

- What adjustments of the criteria and of the form in which they are presented are necessary for a broad diffusion into the shaping of security technologies and measures?

Annex: PRISE forms

Privacy Check for proposal writers

	YES	HOW? ➔PAGE
Relevance of the issue		
Does the proposed technology involve processing of personal data (e.g. data that makes people identifiable)		
Does the proposed technology involve tracking the location or observation of people?		
Core Sphere		
Does the proposal allow / aim at surveillance in homes (assumption: place of retreat and personal life-style; intimate sphere)?		
Does the proposed technology allow / aim at collection or processing of intimate data (data about sex life, sexual preferences, intimate thoughts and conversations, conversations with oneself)?		
Does the proposed technology allow or aim at interaction with partners like spouse, children, lawyer, priest?		
Data Protection Compliance		
Does the technology lack a specification of the purpose of use and data collection or is the purpose given very broad?		
Does possible technology use and data collection and processing require passing a new legal basis?		
Is there a less intrusive means available allowing to achieve the intended result with comparable efficiency?		
Does the technology aim at or allow the collection of sensitive data? (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)		
Does the technology involve linking of data, data fusion or data analysis?		
Does the technology require lifting anonymity of data subjects?		
Is the technology used regardless of whether the individual is suspected of any wrongdoing?		
Is lack of transparency regarding technology use (prior to and/or after use) the default setting?		
Context sensitive trade-off		
Does the proposed technology interfere with human dignity?		
Does the proposed technology interfere with physical integrity of people?		
Does the proposed technology aggravate judicial scrutiny?		
Does the proposed technology facilitate societal security?		
Does the proposed technology aim at crime prevention?		
Does the proposed technology aim at prosecution?		
Is the main field of application fight against… Terrorism		
Organized Crime		
Random Crime		
Does the proposed technology increase individual security against the state (in terms of privacy protection)		
in other spheres (economic, social)		

Privacy Check for Evaluators

	Tools	**Red/green light**
Relevance of the issue		
Does the proposed technology involve processing of personal data (e.g. data that makes people identifiable)		
Does the proposed technology involve tracking the location or observation of people?		
Core Sphere		
Does the proposal allow / aim at surveillance in homes (assumption: place of retreat and personal life-style; intimate sphere)?		
Does the proposed technology allow / aim at collection or processing of intimate data (data about sex life, sexual preferences, intimate thoughts and conversations, conversations with oneself)?		
Does the proposed technology allow or aim at interaction with partners like spouse, children, lawyer, priest?		
Data Protection Compliance		
Does the technology lack a specification of the purpose of use and data collection or is the purpose given very broad?		
Does possible technology use and data collection and processing require passing a new legal basis?		
Is there a less intrusive means available allowing to achieve the intended result with comparable efficiency?		
Does the technology aim at or allow the collection of sensitive data? (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)		
Does the technology involve linking of data, data fusion or data analysis?		
Does the technology require lifting anonymity of data subjects?		
Is the technology used regardless of whether the individual is suspected of any wrongdoing?		
Is lack of transparency regarding technology use (prior to and/or after use) the default setting?		
Context sensitive trade-off		
Does the proposed technology interfere with human dignity?		
Does the proposed technology interfere with physical integrity of people?		
Does the proposed technology aggravate judicial scrutiny?		
Does the proposed technology facilitate societal security?		
Does the proposed technology aim at crime prevention?		
Does the proposed technology aim at prosecution?		
Is the main field of application fight against… Terrorism		
Organized Crime		
Random Crime		
Does the proposed technology increase individual security against the state (in terms of privacy protection)		
in other spheres (economic, social)		

Preliminary list of participants

PRISE User and Stakeholder Workshop:
Guidelines and Criteria for Privacy Enhancing Security Technologies
Vienna, 4th of February 2008

Keynote speakers:

Gus Hosein	London School of Economics and Political Science, United Kingdom
Thomas Petri	Deputy Commissioner for data protection and freedom of information, Berlin, Germany

Participants:

Kurt Einzinger	Internet Service Provider Austria (ISPA), Austria
Simone Fischer-Hübner	Departement of Computer Science, Karlstadt University, Sweden
Gerrit Hornung	University of Kassel, Germany
Niels Christian Juul	Roskilde University, Denmark
Henning Mortensen	ITEK/Association for IT, Telecommunications, Electronics and Communication enterprises, Denmark
John Borking	Borking Consultants, Netherlands
Ian Brown	Department of Computer Science, University College London, United Kingdom
Marit Gjerde	Police Academy, Norway
Kirsten Weinandy	Austrian Federal Ministry of Domestic Affairs, Austria
Mario Savastano	Università degli Studi di Napoli Federico II, Italy
Lasse Øverlier	Norwegian Defence Research Department, Norway
Martin Forster	Center Systems, Austria
Peter Bittner	Humboldt University Berlin, Germany
Bruno Baeriswyl	Datenschutzbeauftragter des Kantons Zürich, Switzerland
Jan Hennig	FoeBuD e.V., Germany
Kasper Skov-Mikkelsen	Trade Organisation for Safety and Security; Denmark

PRISE Advisory Panel:

Caspar Bowden	Chief Privacy Advisor Microsoft EMEA Technology Office, United Kingdom
Gus Hosein	London School of Economics and Political Science United Kingdom
Søren Duus Østergaard	Senior eGovernment Advisor IBM, Denmark
Birgitte Kofod Olsen	The Danish Institute for Human Rights, Denmark
Andreas Schmidt	German Federal Ministry of the Interior, Germany
Michaël Vanfleteren	Legal Adviser European Data Protection Supervisor, Brussels, Belgium

PRISE-consortium:

Johann Čas	Institute of Technology Assessment, Austrian Academy of Sciences
Walter Peissl	Institute of Technology Assessment, Austrian Academy of Sciences
Jaro Sterbik-Lamina	Institute of Technology Assessment Austrian Academy of Sciences
Lars Klüver	The Danish Board of Technology
Ida Leisner	The Danish Board of Technology
Anders Jacobi	The Danish Board of Technology
Mikkel Holst	The Danish Board of Technology
Maren Raguse	Independent Centre for Privacy Protection Schleswig-Holstein (ICPP), Germany
Christine Hafskjold	The Norwegian Board of Technology
Åse Kari Haugeto	The Norwegian Board of Technology