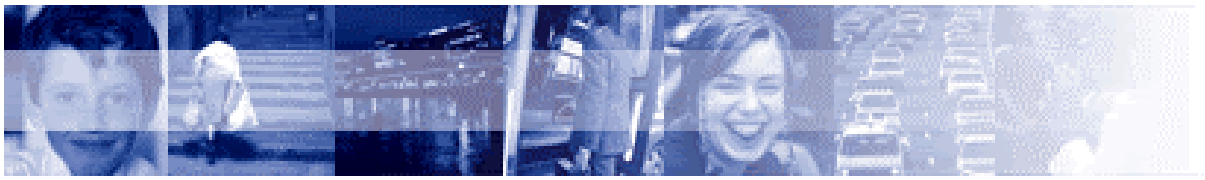
PRISE
privacy • security

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 I

Copenhagen

29 January 2007

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**

User and Stakeholder Workshop Copenhagen - Programme

"Privacy and Security – can you really have both?"

Monday 29 January 2007

10.00 – 18:00

"Eigtveds Pakhus"

Asiatisk Plads 2 G, Copenhagen City

Denmark

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

The chosen participants are the same in both workshops, serving the function as a kind of referencegroup. They are suppliers of security technologies, law enforcement, policy shaping, implementers, users, suppliers of data, data protection authorities, NGOs representing human rights concerns

At the PRISE website http://prise.oeaw.ac.at/ you can read more about the PRISE-project and the workshops.

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

- Privacy issues in security technology development
- Is privacy a barrier for law enforcement?
- How to preserve privacy in the age of anti-terrorism
- How can you balance privacy and inner security?
- How to gain insight into the public reactions to possible future privacy issues (scenarios, impacts and options) – citizen consultation?
- How to develop criteria for privacy enhancing security technologies

Further questions to discuss are found after each Work Package presentation paper.

Preliminary Programme

9:30 – 10:00 Registration, coffee

Plenary:

10:00 – 10:45 **Welcome and introduction**, Lars Klüver, director, The Danish Board of Technology / Johann Čas, PRISE-coordinator, Institute of Technology Assessment, Austrian Academy of Sciences

Short presentation of the participants.

10:45 – 11:30 **Keynotes on Privacy and Security** - different perspectives

Privacy issues in security technology development

- What are the main issues concerning privacy and security from industry's perspective?
- What is the level of awareness of privacy issues in security technology development?
- Is there an added-value (comparative advantage) for security industry in privacy enhancing systems design?

by Peter Munday, Thales Research and Technology (UK)

Is privacy a barrier for law enforcement?

- What are the main issues concerning privacy and security from a law enforcement perspective?
- Directive 1995/46/EC allows for restriction of privacy in order to safeguard public security. What limits exist to this restriction of privacy? Could this provision lead to a state of zero privacy?
- As the actual intensity of privacy impact of a security technology is determined by national police law, what approach fostering privacy enhancement on a European level is possible at all?

by Hans Jørgen Bonnichsen, Former Head of Operations in Danish Security Intelligence Service

Privacy in the age of anti-terrorism

- What are the main issues concerning privacy and security from the human rights perspective?
- Will there any privacy be left to European citizen?
- Do we need privacy at all?

by Ian Brown, Department of Computer Science, University College London

11:30 – 12:30 Open discussion

12:30 – 13:30 Lunch

Plenary:

13:30 – 13:45 Introduction to the Workshop Groups

In groups:

13:45 – 15:30 Three parallel Workshop Groups

Participants choose themselves which workshop group to participate in.

The purpose of each group is to give feed back to the guiding questions that have been presented in the workshop paper. We would like the participants in the workshop to each give an introductory comment (maximum five minutes) on what he/she think is particularly important in the further work on the topic at hand.

Workshop A: How can you balance privacy and inner security?

Opportunity for short comments from the participants on what issues he/she thinks is important to consider in the further PRISE-project.

Presentation of PRISE-work and questions to be commented on by the workshop group (10 min.)

Mapping of privacy impacts and options for privacy enhancing design
by **Maren Raguse**, Independent Centre for Privacy Protection Schleswig-Holstein (ICPP), Germany

Facilitator / rapporteur: Ida Leisner and Maren Raguse

Workshop B: Scenarios - Asking the citizens

Opportunity for short comments from the participants on what issues he/she thinks is important to consider in the further PRISE-project.

Presentation of PRISE-work and questions to be commented on by the workshop (10 min.):

Development of implementation scenarios
by **Christine Hafskjold**, The Norwegian Board of Technology

and

Participatory Technology Assessment of Scenarios. Questions to be posed to the citizens
by **Anders Jacobi**, The Danish Board of Technology

Facilitator / rapporteur: Christine Hafskjold and Anders Jacobi

Workshop C: Criteria for privacy enhancing security technologies

Opportunity for short comments from the participants on what issues he/she thinks is important to consider in the further PRISE-project.

Presentation of coming PRISE-work and questions to be commented on by the workshop (10 min.):

Criteria for privacy enhancing security technologies. What is needed to be known or done before introducing new security technologies?
by **Walter Peissl**, Institute of Technology Assessment, Austrian Academy of Sciences.

Facilitator / rapporteur: Walter Peissl and Johann Čas

15:30 – 16:00 Break

Plenary:

16:00 – 16:45	What we learned from the workshops - by the rapporteurs
	Report from each of the three Workshop Groups, collectively, all group members can contribute
16:45 – 17:00	Conclusions from the day, Lars Klüver and Johann Čas
17:00 –	Farewell drinks
19:30 –	Dinner for members of the Advisory Panel and the PRISE-partners at **Nyhavn 71 Hotel**, Nyhavn 71, København City, www.71nyhavnhotel.com

Practical information

PRISE - Workshop: Privacy and Security – can you really have both?"

Monday 29 January 2007, 10 - 18

The conference center

"Eigtveds Pakhus"

Address
Asiatisk Plads 2 G
1448 København K
Tlf. + 45 33921601/02, + 45 33921509/10
Telefax: + 45 33921631, + 45 33921773
E-mail: eigtved@um.dk

Reception
Tlf. + 45 33921601/02

See the address on the map: http://www.euroave.com/maps/01map.php?xcity=copenhagen&glj=709

The Conference Center is owned by the Ministry of Foreign Affairs of Denmark, near to the Danish Parliament and even nearer, just a few metres from the water, the canals of Copenhagen.

Built in 1748, original it was a busy warehouse, today respectful restored and meeting place for international activities.

More about Denmark: http://www.visitdenmark.com/siteforside.htm

Transport and Accommodation
Accommodation and travel expenses can be covered by the project budget. At the PRISE website you can find a reimbursement form: http://prise.oeaw.ac.at/workshops.php

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 **Anne Funch Rohmann**, project manager, The Danish Board of Technology, e-mail afr@tekno.dk, direct telephone + 45 33 45 53 64, reception telephone +45 33 32 05 03.

Papers presenting the Work Packages in PRISE

Overview of Security Technologies

The Overview of Security Technologies is the main deliverable of Work Package 2 of the PRISE project. The purpose of the report is to constitute the basis for the further work in the project – in particular with mapping privacy implications in Work package 3 and developing scenarios for the participatory technology assessment in Work package 4.

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.
- 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.
- We will only discuss 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 an on-going R&D project.

Technology model

Even with the criteria presented above, the field of security technologies and means is rather large. In order to structure our findings, we divided the technologies in four groups. Within each group we classified the technologies: *Basic technologies* are the foundation of the security *Application areas*. To illustrate some of the application areas we give a number of *System examples*. These examples are known real-world implementations of the application areas.

The idea of the *technology model* is to show that security applications draw on many different basic technologies, and in doing so they also inherit the risks to privacy intrinsic to those technologies. For example: Because Machine Readable Travel Documents (MRTDs) are based on communication technology, sensors, data storage and biometrics, this application faces privacy challenges related to all these basic technologies.

The strength of this model lies in the ability to analyse application areas that are still at the research stage, and even future technologies that currently only exist as ideas. If these applications combine one or more of the basic technologies described, they may also inherit the privacy properties of these technologies.

This will make it possible to analyse these technologies' privacy impact, and thus relevance to the PRISE project.

Basic technologies

The basic technologies are technologies that can be found in many areas of society – not only in security applications. It is, however, important to look more closely at these technologies and their privacy implications in order to better understand the privacy implications of the application areas and system examples.

The first basic technology presented in this report is *Communication technology*. Communication is a prerequisite for almost all application areas: There is communication between sensors and readers, between local computer systems and central databases etc. The main privacy challenge is that communication containing sensitive data may be intercepted or that communication may take place remotely and unobserved. Communication technology can also reveal the location of a person – either directly or through further analysis of the communication data. In addition, communication between applications that use radio frequency identification (RFID) may not be transparent– the person involved will not be able to check what is communicated and if communication is taking place at all.

The following communication technologies are described:

- Public Switched Telephone Network (PSTN)
- Mobile telephony
  - Eavesdropping
  - Technical identification of telephones and communication equipment
- Communication over the Internet Protocol
  - Packet sniffing
- Locating systems
  - Location through GSM Base stations
  - Satellite based positioning systems
    - GPS
    - Galileo

Biometric technology can be used to identify individuals by using their biological or behavioural characteristics. The most commonly used biometrics are facial characteristics and fingerprints. Biometrics affect privacy in a number of ways:

- Biometrics relate to behavioural and physiological characteristics of a person and can be used to uniquely identify that person.
- Biometric data like fingerprints and DNA samples may be collected without the data subject's knowledge.
- Biometrics can reveal intimate information like race, ethnicity, mood – and in the case of DNA – hereditary factors and medical disorders.
- Biometric systems are vulnerable to spoofing. Because there is such a strong connection between the data subject and the biometric, it is very difficult for a victim to prove misuse by an impostor.

The following biometrics and related technologies are described in the report:

- Fingerprints
- Facial characteristics
- Iris
- Automatic identification
- DNA profiling

Sensors can be found in a number of applications, ranging from CCTV (electro optical sensors), to ID cards containing integrated circuits. The main privacy challenge related to sensors is that the data subject normally don't know that his or her information has been registered (e. g. image captured through CCTV, conversation captured through a microphone or RFID chip read by a reader from a distance).

The following sensor technologies and applications are described in the report:

- Sensors used for scanning applications
  - Sensors for ionising radiation
  - Terahertz technologies
- Electro-optical sensors
  - Closed Circuit Television (CCTV)
  - Intelligent Video Management/Automatic monitoring
- Acoustic sensors
  - Bugging
- Unmanned Arial Vehicles (UAVs)
- Radio Frequency Identification (RFID)
  - Machine Readable Travel Documents (MRTDs)
  - ID cards

Data storage and the analysis of the data stored are the final basic technologies described in this report. The storing of personal data provides a number of privacy challenges. When different pieces of data about a person are linked together, more information is revealed than when the information items are only available separately. This challenge increases when several data sources are linked together and analysed (Data mining, search) often without the data subject's knowledge. Databases are also vulnerable to function creep – the use of data for a different purpose than it originally was collected for. Central databases are also exposed to breaches in security.

The following technologies related to data storage are described:

- Database systems
  - Data Retention
  - Border control systems
  - The exchange of passenger information in international travel
- Data Mining
- Search technology

Guiding questions for the workshop to discuss

Do the criteria that security technologies and means should fulfil in order to be relevant to the project seem reasonable? Or will they limit the project because areas of technologies are excluded? If so; why?

Is the described technology model an adequate tool to analyse the privacy impact of complex technologies? And even technologies that are still in the research stage?

Do the described technologies constitute an overview of relevant security technologies for Europe today? If not – what technologies or application areas, in your opinion, are missing?

Mapping of Privacy Impacts and Options for Privacy enhancing design

The context and scope of Work Package 3 in PRISE

Work Package 3 aims to analyse the security technologies chosen in Work Package 2 with regards to their impact on the privacy of EU citizens or other people entering or living within EU Member States.

Privacy impacts will be identified according to existing and applicable legal regulations and the legal remedies of such impacts will be presented and evaluated with respect to an adequate protection level for citizens, inhabitants and visitors to the EU.

The choice of security technologies in Work Package 2 together with the privacy impact evaluation in Work Package 3 will serve as a backbone for the later WPs giving reasons for establishing privacy standards for security technology research.

Work Package 3 will result in technical, legal and organisational proposals fostering not only privacy compliant use and development of security technologies but more so privacy enhancing design of these technologies. Proposals will be provided where additional protection should be put in place and limitations of usage of security technologies will be outlined.

These results of Work Package 3 will serve as major input for Work Package 6 – Criteria for Privacy Enhancing Security Technology.

Results from Work Package 3

Work Package 3 does focus on a legal analysis of the impact of security technologies on European citizens' right to privacy and will conclude in proposals on what technical features in security technology will ensure privacy enhancement, what legal requirements will lead to a balanced abidance of the citizens' civil rights and finally, how to operationalize these legal and technical proposals in projects receiving Framework 7 funding.

Since the September 11 attacks in 2001 not only the United States endorse the view of a raised threat by terrorists and have thus significantly increased 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 so-called anti-terror laws and have instituted repressive measures in the name of fighting terrorism. These legislative steps aim at detecting conspiracies to terrorist acts at an early stage of planning. In order to achieve this early locating of terrorists the legislative measures seek to cover all areas of possible terrorist planning: border control to prevent entry of known terrorists, detecting their communication, detecting their whereabouts and social network, interrupting their cash flow and the protection of potential targets like critical infrastructure or air travel.

In order to be in a position to already detect early plans of attacks or enable a later analysis of networks and planning, European governments argue it is necessary to collect information on individuals early (even without a sufficient suspicion of a criminal act 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 include eavesdropping of telecommunication, 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, extension of video surveillance in public places or control orders allowing electronic tagging of suspects.

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 adoption of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. It introduces inter alia measures to improve information exchange for DNA and fingerprints. All Member State of the European Union may join the convention. The Contracting Parties aim to incorporate the provisions of the convention into the legal framework of the European Union.

In this context police and secret service need new or improved technologies to meet up with the technical state of the art which criminals and terrorists use more than ordinary citizens with the intention to disguise their traces, plans and communication. It is for this reason that a focus of the EU's Framework 7 Programme will be on security technologies research.

The actual application of a security technology is determined by national law of the Member States and this use of security technologies and the definition of powers of intervention and investigative methods determine the level of privacy impact for citizens subject to the investigation or screening.

It has been claimed that Human Rights have been among the first casualties of EU countries' efforts to strengthen their anti-terrorism powers.

A focus of the legal research in Work Package 3 is not to suggest changes in national police law of the Member States as the perspective of PRISE is a European one. Article 13 of Directive 1995/46/EC states that the right to privacy may be restricted when such a restriction constitutes a necessary measures to safeguard public security and the prevention, investigation, detection and prosecution of criminal offences. In this context the Legal Report discusses 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 comply with general privacy principles which due to transposition of Directive 1995/46/EC are a common ground for Member States. They 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.

The Legal Report thus does not stop at an overview of necessary features security technologies need to comprise. As the level of privacy impact is determined by legal provisions, a product which might enable a privacy enhancing use may according to national police law still be used in a far more infringing way than intended or foreseen by its developers. Also, national governments may ask for a customized technology, very often research is even triggered by demands of national governments acting as contractors.

The German constitutional court has ruled that the right to privacy embraces a core which must not be violated. In the Legal Report a number of relevant cases are presented and the report describes that 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.

Main focus of future work / guiding questions

The aim of PRISE is also a discourse on ethical standards of EU funding. PRISE will in its Proposal Report in Work Package 3 discuss whether research projects aiming at very privacy infringing products applying for Framework 7 funding should be rejected for ethical reasons and will suggest the introduction of an ethics tests at an early stage of the funding application process.

Another organisational proposal PRISE will present is the introduction of a Data Protection Management process into companies working on research and development of security technologies. Data protection compliance needs to be an integral part of the development process and checks in all stages of development (plan – build – run – customize) should be implemented.

Guiding questions for the workshop to discuss

Directive 1995/46/EC allows for restriction of privacy in order to safeguard public security. **What limits** exist to this restriction of privacy?

As the actual intensity of privacy impact of a security technology is determined by national police law, **what approach** on a European level is possible at all?

Development of implementation scenarios

The PRISE-project has created scenarios in Work Package 4. The scenarios are partly based on previous work in the project (in particular Work Package 2) and the work of a group of external experts. The scenarios are a major input to the participatory activity in the project. The credible and thought provoking scenarios are based on the knowledge of existing security technologies and their impact on privacy.

The scenarios will be presented to groups of lay people in different European states. The scenarios aim at giving the lay people insight into different security technologies and how they can be applied in everyday life in a near future. The Prise-project try to address different approaches to the technologies, both from a user point of view, and in the society.

See the draft version of the scenarios in the separate document – **"D 4.1. Scenarios"** - or at the PRISE website http://prise.oeaw.ac.at/

Guiding questions for the workshop to discuss

Are the scenarios credible?

Do they seem balanced?

Is the selection of technologies and situations right? Are there other technologies/situations that should be included?

Asking the citizens – the interview meeting

"Human factors" play a big role when shaping and applying security policies. As a part of the PRISE project, citizen participatory activities - each involving 25-35 citizens - will be carried out in 5 European Union member states and in Norway. The purpose is to establish a combined quantitative and qualitative insight into public perceptions of security technology and privacy.

Work package 5 of the PRISE project is the participatory activity, which will provide insight into the public perceptions and citizens' preferences on the scenarios that are developed in work package 4. The purpose of work package 5 is to provide input for the further development of criteria for privacy enhancing technologies, which will take place in work package 6.

The participatory methodology for work-package 5 is "the interview meeting". The interview meeting includes a questionnaire and a subsequent group interview. In the following the interview meeting method is described and three guiding questions for the workshop is posed.

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 representative method but it aims at including a diverse group of citizens who cover a broad spectrum of demographic criteria such as age, sex, religion, 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 under exploration. However, prior to and during the meeting, the participants are informed about the advantages and disadvantages of the technology so that they share a balanced and factual starting point. In the PRISE project, this information is based on the scenarios developed in WP4 and the dilemmas that these scenarios focus on.

The interview meeting method employs a combination of a questionnaire and group interviews. These two methods 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. Interview meetings are particularly suitable in cases where:

- There are complex issues (technically complex and/or ones posing a dilemma)
- Prior public knowledge is limited
- An ethical dimension is involved

The issues at stake in the PRISE project make the interview meeting a suitable method for involving citizens.

Purpose

The purpose of the interview meeting is to gain insight into the various notions, wishes, concerns and attitudes prevalent among the interviewees. The interview meeting must provide an indication of the general views of the interviewees and the underlying reasons for these. The purpose is thus not to conduct an actual opinion poll. The interviewees' answers provide insight into:

- fundamental attitudes towards a given technology
- the underlying reasons for these attitudes

- the variety of arguments that exist among the interviewees
- how citizens weigh different arguments and ethical principles against one another

Within PRISE, focus is of course on security technology and how it can be developed and applied in a way that does not threaten privacy. The purpose of the interview meetings is to get citizens' feedback on the scenarios (developed in WP4)

Procedure of the interview meeting

The interview meeting is held in the evening and takes the form of a three-hour after-work meeting. Two to three weeks before the interview meeting, a short informational background material about the topic is sent to the participants along with the scenarios developed in WP4. The introduction material and the scenarios will give the participants an insight to security technology and privacy issues, as well as the dilemmas connected to the subject and what is for and against the different technologies.

In addition to the written material, the meeting begins with an introduction to the topic, with focus given to the advantages and disadvantages of the technology to be discussed.

The interview meeting begins with an introduction. The introduction is normally presented by one or more experts in the field. Following this, participants can put clarifying questions to the presenters.

After the introduction, participants are handed a questionnaire. Participants have 30-45 minutes in which to complete the questionnaire. The questionnaire focuses on the same dilemmas as the scenarios. Questions can be put to the organizers or the experts throughout the session if need be.

After the questionnaire, participants are divided into four groups of 6-9 people and group interviews are subsequently carried out. The group interviews focus on the same topics as those of the questionnaire. Interviews are tape-recorded and follow an interview guide but smaller variations are allowed. Interview questions are about 1) reasoning behind the answers given in the questionnaire and 2) the relevance of the questionnaire. The interviews are monitored by an interviewer whose task is to ensure that all of the participants are heard and that all themes and questions are discussed and answered. The group interviews last one hour.

An interview meeting provides both quantitative and qualitative results. Questionnaire answers provide comparable, measurable, quantitative results and the group interviews are used to gather the more qualitative results that give nuance to those of the questionnaire. Comparison and analysis of the two sets of results offer a balanced indication of public attitudes towards a given technology. After the meeting the group interviews are transcribed and statistics on the questionnaires are prepared. In the final analysis the quantitative and the qualitative data is combined in order to assess which criteria are relevant and why and how far the consensus reaches among the citizens.

The results will basically give insight into the citizens' priorities and there evaluation of dilemmas connected to security technology and privacy. The citizens will give their unique input from their "citizen logic". The six national reports will be compared in a synthesis report made by the WP5 leader and reviewed by the other five partners/subcontractors.

Guiding questions for the workshop to discuss

What are the strengths and weaknesses of the interview meeting method for asking the citizens?

What dilemmas, technologies and situations from the scenarios are most important to discuss at the interview meetings?

What are the implications of comparing results from six different countries?

Criteria for privacy enhancing security technologies

Objectives

Workpackage 6 of the PRISE project will:

- identify best practice models regarding the privacy friendly design and implementation of security technologies, based on the results of workpackage (design principles) and workpackage 5 (participatory technology assessment)
- transform these models into different sets of criteria for research programmes (incorporation into call and evaluation guidelines), industry projects, evaluation by data protection authorities, implementation processes, legislation, regulation and execution of security policies and
- discuss and test these sets of criteria for applicability within the user and stakeholder panel

Questions to help identify criteria

1) What sets of criteria do exist?

In addition to the inputs from other work packages workpackage 6 will undertake an analysis of existing criteria catalogues and sets related to the objectives of PRISE, specifically on criteria for PETs (Privacy Enhancing Technologies). Examples for existing criteria are anonymity, pseudonymity, unlinkability, unobservability. These criteria may be achieved by methods of data minimisation, data protection and data protection management. Taking the desktop research approach as starting point, workpackage 6 will scrutinize these sets for common criteria, which are applicable to security technologies and their employment.

By early application of privacy enhancing criteria in the design phase of security technologies and research it is more likely to create a competitive advantage for European security industries. With respect to European attitudes the chances for acceptance of security technologies will be higher by taking into account the social dimension beforehand. Furthermore, early integration of privacy enhancing features into systems and products will minimize possible failures on the market later on and therefore avoid economic troubles.

2) What are the criteria for criteria?

We aim at a number of “sets of criteria” for different actors (target groups) in different “application environments”. This means criteria have to take into account that different actors have different tasks to fulfil and therefore require different sets of criteria to fulfil their respective tasks in a privacy enhancing manner. This also counts for different phases of technology or systems development. In early phases of research and development other types of criteria may be applicable than in the implementation phase or when the technology is being used. The target audience for PRISE is first European research and funding policy. Furthermore, we will try to attract research, industry, data protection authorities and users of security technologies. Therefore the criteria are supposed to be as clear as possible, practical and unambiguous. Last but not least, it should be possible to control compliance with the criteria.

Criteria will be analysed at least in three different dimensions: technical, organisational and legal. They will be interlinked with general principles and made applicable for different actors in their respective field of implementation and responsibility.

Criteria	From principles	to	most concrete application
Technical	→ principle X, Y, Z	→ security technology A, B, C…	→ application environment
Organisational	→ principle X, Y, Z	→ organisation (enterprise, public user, technology developer, DPAs…)	→ organisational setting
Legal	→ principle X, Y, Z	→ European law	→ national rules

3) What is the privacy-security dilemma all about?

For analysing criteria one possible model will be the trade-off between privacy and security. It will be part of the Work Package to discuss this dilemma. Most of the discussion on privacy and security implicitly uses the model, which says that more security is only available via more surveillance, hence at the cost of privacy. We will have to analyse whether this model is useful and the underlying equation is correct. If so, we will try to figure out fields of application where more security technologies (surveillance, measuring, controlling, sensing etc.) may enhance societal security with a minimum of detraction of privacy.

The overall goal of this Work Package is to overcome the "privacy-security dilemma" (where it exists).

There are two guiding questions:

- Does less privacy automatically lead to more security?
- Is more security possible with the same (or even higher) level of privacy?

4) What levels of protection do we deal with?

In Europe there is a legal framework for data protection in place (Directive 95/46/EC). Actually this is the limit for all activities concerning personal data. The main challenge we are facing is that in Article 3 it says: … 2. This Directive shall not apply to the processing of personal data:
– in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law, …

And Art. 13 of Dir. 1995/46/EC states that: Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for … when such a restriction constitutes a necessary measure to safeguard – national security, …the prevention, investigation, detection and prosecution of criminal offences, …

However, privacy is a fundamental right, which – under certain conditions only – may be traded-off with other societal needs. Furthermore it is a prerequisite of democratic societies and basically a fundamental psychological need of individuals. Questions to discuss will be how to define the limit for security

technologies in terms of privacy infringement and how to deal with the trade-off between privacy and security.

Basically we deal with three levels of protection. Systems may be:

- compliant to (national) regulation for inner security and law enforcement or
- data protection compliant or
- privacy enhancing

5) How could a scheme for privacy compliant security technologies in Europe look like?

As stated above, there is a limit to trading-off privacy to security. Main arguments will be found in philosophical as well as political science theories of democracy and their basic assumptions. Therefore we will have to state minimum criteria, which a system should meet at all cost.

Having this in mind, we will argue for a step-by-step approach:

- Baseline of systems development (the "limit")
- Data-protection compliant systems design
- Context sensitive trade-off between potential security gain and privacy loss (intrusion to privacy needs to be justified and alleged gains in security must be substantiated or at least be very likely)
- Privacy enhancing systems design (the step further)

For research funding, we think there are good arguments supporting a kind of precautionary principle. This means that we should be rather careful in accepting privacy infringements. All systems should basically be fully privacy compliant. If they are not there need to be good arguments in terms of security gains (e.g. projects have to prove security enhancement first, if they want to incorporate features or procedures that potentially infringe users or citizens privacy).

Guiding questions for the workshop to discuss

Are the 5 questions to help identify criteria adequate to fulfil the task?

How would you answer these questions?

What is missing?

Preliminary list of participants

PRISE User and Stakeholder Workshop:

"Privacy and Security – can you really have both?"

29 January, Copenhagen

Keynote speakers:

Peter Munday	Chief Technical Consultant	Thales Research and Technology (UK)
Hans Jørgen Bonnichsen	Former Head of Operations	Danish Security Intelligence Service
Ian Brown	Dr.	Departement of Computer Science, University College London

Participants:

Caspar Bowden	Chief Privacy Advisor	Microsoft EMEA Technology Office, UK
Armgard von Reden	Dr., Chief Privacy Officer	IBM Europe, Middle East and Africa
Kurt Einzinger	Dr.	Internet Service Provider Austria (ISPA)
Simone Fischer-Hübner	Prof. Dr. habil.	Departement of Computer Science, Karlstadt University
Ralph Bendrath	Dipl. Pol.	Collaborative Research Centre 597, "Transformations of the State", University of Bremen
Rikke Frank Jørgensen	E.MA/MA, E.MA, teamleader	The Danish Institute for Human Rights
Gerrit Hornung	Director of Provet, Dr. LL.M	University of Kassel, Germany
Reyes Munoz de la Torre Crespo	Head of Legal Services, Mag.	Data Protection Agency of Madrid, Spain
Walther Grosinger	Mag.	Federal Ministry of the Interior, Vienna, Austria
Niels Christian Juul	Associate Professor, Ph.D	Roskilde University, Denmark
Leif T Aanensen	Deputy Director General	Department of Inspection and Information Security, Norway

Henning Mortensen	Consultant	ITEK / Association for IT, Telecommunications, Electronics and Communication enterprises, a Confederation of Danish Industries
John Borking	Privacy Adviser	Borking Consultants, member of the Dutch Data Protection Agency, EU-adviser

The PRISE Advisory Panel:

Søren Duus Østergaard	Senior eGovernment Advisor	IBM, Denmark
Leo Hennen	Dr.	Institute for Technology Assessment and Systemsanalysis (ITAS), Research Center Karlsruhe
Birgitte Kofod Olsen	Director of Department, Ph.D	The Danish Institute for Human Rights
Andreas Schmidt	Dr.	German Federal Ministry of the Interior, Berlin
Michaël Vanfleteren	Legal Adviser, LL.M	European Data Protection Supervisor, Brussels

The PRISE-consortium:

Johann Čas	Co-ordinator, Institute of Technology Assessment, Austrian Academy of Sciences
Walter Peissl	Deputy Director, Institute of Technology Assessment, Austrian Academy of Sciences
Lars Klüver	Director, The Danish Board of Technology
Ida Leisner	The Danish Board of Technology
Anders Jacobi	The Danish Board of Technology

Anne Funch Rohmann	The Danish Board of Technology
Marit Hansen	Independent Centre for Privacy Protection Schleswig-Holstein (ICPP), Germany
Maren Raguse	Independent Centre for Privacy Protection Schleswig-Holstein (ICPP), Germany
Tore Tennoe	Director, The Norwegian Board of Technology
Christine Hafskjold	The Norwegian Board of Technology
Åse Kari Haugeto	The Norwegian Board of Technology

Presentation of the keynote speakers

Peter Munday graduated from Cambridge University in 1970 with a first class degree in mathematics, and in 1975 obtained an MSc in electronics from Southampton University. He joined Racal (now Thales) Research as a Development Engineer in 1975. He has been with the company since then and is now a Chief Technical Consultant.

He is experienced in the design, development and evaluation of military and civil electronic systems, in particular radio and security systems. He invented the synchronisation system for the Racal Jaguar -V frequency hopping radio. He worked on development of the TACS and GSM cellular systems, including the radio interface technical standards. He has provided consultancy on a number of programmes in ESM and ECM, UAV surveillance, air defence, and port and container security. He was the co-ordinator of the ESSTRT supporting activity on security roadmapping in PASR2004.

Thales is a leading international electronics and systems group, serving defence, aerospace and security markets worldwide, supported by a comprehensive services offering. The group's civil and military businesses develop in parallel to serve a single objective: the security of people, property and nations. Leveraging a global network of more than 20,000 high-level researchers, Thales offers a capability unmatched in Europe to develop and deploy critical information systems. Thales employs 70,000 people in 50 countries and generates annual revenues of more than EUR13bn.

Hans Jørgen Bonnichsen is a Senior Law Enforcement Adviser. He has retired as Detective Commander, Head of Operation of the Danish National Intelligence and Security Service. He has worked 41 years in the Danish National Police, 20 of which in the National Commissioner’s Office as deputy chief. The latest nine years was with the Danish Security Intelligence Service as Head of Operation against espionage, extremism and terror.

Ian Brown is a senior research manager at the Communications Research Network and a senior research fellow at University College London, where he teaches a range of computer science courses. His main professional interests are in public policy issues around information and the Internet, as well as the more technical fields of information security, networking and healthcare informatics.

Dr. Brown is a fellow of the RSA and BCS, and advises a number of NGOs, research projects and companies. In all these roles he has worked on a wide range of information policy issues such as critical infrastructure protection, surveillance, privacy, export controls, copyright and electronic voting. Reports and papers on these issues have been cited in both Houses of Parliament and parliamentary briefing notes. They have also been covered on BBC2, Channel 4, CNN, CBC, the BBC World Service and in numerous newspapers and magazines. This work has led NOP to name him as one of the 100 most influential people in the development of the Internet in the UK over the last ten years.