PRISE
privacy • security

Security Research

PASR

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

Minutes from

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**

Minutes from the plenary session

Privacy control must not slow us down

The keynote speech by Peter Munday pointed to the dilemma of protecting privacy in situations where fast data sharing is important for security reasons.

Security technologies must provide a way to find “a needle in a haystack” – the one terrorist or criminal among millions of people on trains, aircrafts or in shopping malls. In many cases it is a matter of urgency, and there might not be time to get the necessary permissions.

Mr. Munday emphasized that these technologies must be reliable and enable finding the bad guy without hindering the good guys. He described that many technologies are close to their theoretical limit of performance and a major help when aiming at ensuring security of the state and individuals will be data fusion, data mining and data sharing. This could improve performance of the technologies and fusing data would reduce false detection rates.

Storing information captured by sensors in a database enables analysis patterns of activities and detection of anomalies (e.g. "same" vehicle in 2 places at same time). According to Mr. Munday, there may be a problem regarding the possible access by corrupt officials. A solution to this problem is the implementation of access rules (purpose for which law enforcement agent may access data stored in a database), storage in tamper-proofed systems (write once – read many) and an audit trail.

Some participants questioned the need for immense and fast data sharing, referring to the many false positives that can be expected and have already occurred in recent anti-terror investigations. An example was the young man killed in London being wrongly suspected of planning an act of terror. Still several of the participants together with Mr Munday found, that data sharing and data mining are important measures in fighting terror, even though data mining is exaggerated in value.

It was commented that in the medical environment, the need for speed in emergency situations has been handled for many years. Systems can be overridden in emergency situation, but the anomaly has to be thoroughly documented, so that it can be assessed at a later stage.

It was thus suggested to raise the question in the PRISE project whether it is possible to define legal requirements, technical possibilities and potential side-effects and safeguards for accessing databases and that will enable fast data sharing.

Mr. Munday concluded his presentation by admitting that the level or awareness of privacy issues in security technology development is growing but could be improved. In this context the need for system level design is forcing an early focus on privacy issues.

It was commented that there are ways of analysing data in an anonymous way. It is technically possible to compare data from many sources, in search of matching attributes. Matching the partial identities of individuals who might try to disguise their identity in order to then perform a profiling process and to aggregate information can be done in a privacy compliant manner. Adding anonymity could be a possible privacy protection measure: Lifting anonymity should only be done when suspicion is documented, and only after a court warrant has been granted.

With regards to an added value for the security industry when it comes to Privacy Enhancing Technologies Mr. Munday stated that authentication and encryption are vital components of many security systems. Other techniques like anonymity will be developed if there is a market for them.

Forcing the market to protect privacy – legislation and public procurement

Privacy is not a barrier for law enforcement, according to keynote speaker Hans Jørgen Bonnichsen.

Mr. Bonnichsen further stated that the core of privacy has been invaded in today's society. Citizens take part in this by using technologies like ATMs or cell phone which leave electronic traces ready for matching and profiling.

He noted that political systems "under pressure" might not be ethically robust and don't put enough focus on protecting their citizens' civil rights. Mr Bonnichsen emphasized that secret services should not give way to a general mistrust towards society. Instead, Mr. Bonnichsen concluded, we must learn to live with the threat of terror which is not a greater risk to life than driving a car. He finally reminded the participants that waiving civil rights is the foremost aim of terrorism.

It was discussed if privacy could be a competitive advantage, or if the price would be too high to expect private business to voluntarily improve privacy. To what extent could legislation force the market to take privacy serious? Industry will respond positive to knowing what standards they should live up to, but then legislation must not be too complicated to translate into business terms.

In the financial sector privacy and security is a prerequisite for being in business. Other types of business have to learn – or be pushed to integrate privacy compliance.

Public procurement could be stressed as another way of forcing the market. If the customers demand privacy compliant solutions, the industry is much more likely to develop such solutions.

Privacy ever-more fundamental in the information age

According to keynote speaker Ian Brown citizens' right to make mistakes, to learn and to grow is at risk if more data from commercial sources keep being aggregated, linked and analyzed.

Citizens might in the future try to show inconspicuous behaviour – meaning they might try not to get in the focus of automated detection technologies scanning public areas like streets or malls for unusual behaviour. Mr. Brown stated a fundamental psychological need for some control over how we are seen by the world as an expression of autonomy and dignity.

Discussing the relation of privacy and security Mr. Brown emphasized that privacy is only an enemy of pseudo-security measures that mistake compiling vast lists and databases with security. The relation of privacy vs. security can, according to Mr. Brown, not be measured on a scale resulting in the finding "less privacy – more security". The belief that data mining will simply pop out terrorists was called a fantasy by the speaker. Attempts to detect terrorists or unveil plots to terrorist attacks are difficult as there is no well-defined profile of possible terrorists and attacks are very rare. He sited Bruce Sneier, saying that taken together, these facts mean that data-mining systems won't uncover any terrorist plots until they are very accurate, and that even very accurate systems will be so flooded with false alarms that they will be useless.

It was stated that the remark that a privacy impact analysis would have to be budgeted for indicates that privacy is still considered an "extra" which currently is not part of planning and defining the functionality of security technologies.

In closing, Mr. Brown cited IBM Chief Scientist Jeff Jonas with the words "Techniques that look at people's behavior to predict terrorist intent are so far from reaching the level of accuracy that's necessary that I see them as nothing but civil liberty infringement engines".

Balance and scope of the project

Participants found the PRISE project as such very important in addressing the need for European regulation, planning and action towards privacy infringing use of security technologies. As further discussed in workshop A, many of the participants questioned the idea of balancing privacy with security, stating that the right to privacy is also aiming at a state of security for the individual to be free from state interference where possible.

Concerning awareness, the different cultural traditions in European member states were mentioned.

(Some participants suggested to also analyze nanotechnologies and ambient intelligence in the project, and to include health care sector in the applications. During the discussion participants endorsed the concept of PRISE trying to extract some general principles/criteria for any technology/application covered by the 4 basic technologies).

Data minimisation and proportionality: is it necessary to increase the haystack

Many participants wanted the PRISE project to support the proportionality principle. Today implementations too often strongly affect the majority of innocent people, and many new technologies taken into use create new databases to be protected.

The haystack [terrorist – needle in data haystack] increases dramatically in this way, without any control and not enough consideration to what security effect will be gained. Increasing the haystack won't make finding a criminal easier. So far increasing the amount of data has not been proven effective to solving more criminal cases or terrorist attacks. An evaluation of the effectiveness was considered necessary. As criminals well know how to disguise their steps, limitations will be on innocent citizens who don't think they have anything to hide.

Attention was drawn to a consideration of a global balancing of investment, wherein investing money in other places than security technology would save more lives than inefficient security technologies looking for terrorists could.

Criteria require that the legislation on data protection is taken into account from the beginning of the process of developing new security technologies.

Since the designers of the technologies hardly ever think of privacy issues, it is important to force them by including corresponding criteria for funding research.

Criteria to avoid "halfbaked" technologies

Some argued that to aim for a zero risk society is not useful. We have to accept some risks, and also prioritize investments that will lead to the benefits we want – a balance that should also be considered. This approach will include assessing the effectiveness of the technologies, and thus avoid trying out technologies that are not thoroughly assessed ("halfbaked") on a large scale.

The quality criteria have to be clear in assessing privacy impact. A criterion could be to suggest a frequent evaluation of the security mechanism of the technologies and their application.

Raising awareness of privacy

Many participants subscribed to the perception of a lack of understanding of privacy in society but also among stakeholders and developers of security technologies. The need for guidance was stated. A possible approach would be for data protection authorities to invest in people who can advise companies on privacy compliance and enhancement.

Currently, no political value in promoting privacy was discovered by politicians as public opposition to privacy infringing measures has remained on a small and therefore negligible level for politicians. Only if the risk of losing votes is perceived, decision-makers attention can be drawn to ensuring privacy.

E-immunity shield

The University of Leuven will introduce a new privacy by design approach as an alternative to PETs. They are developing a concept of e-immunity, by simulating the human body immunity system. A shield around a person will sense the presence of sensors and judge if one of them could be an attacker.

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

Balance between Security and Privacy

A short welcome was followed by a presentation on the legal work in PRISE and some first proposals on how to achieve privacy enhancing design of security technologies.

It was argued that the level of privacy impact caused by security technologies is determined by two factors: the technological features of a technology and the legal framework regulating its application by police and secret service.

In order to assess the privacy impact of the many existing technologies, PRISE has identified four underlying basic technologies to which all analyzed security technologies can be mapped. The privacy impact inherent to the basic technologies will thus be found in the application combining one or more of the basic technologies. Furthermore, a combination of basic technologies will in many cases increase the privacy impact.

The legal requirements on the actual use of security technologies are mainly regulated in the national police laws of the Member States. The biometric passport, the data retention directive and for example anti money-laundering laws are measures introduced by the European Union to combat organized crime and terrorism. While the collection of information in the cause of an investigation is subject to national legislation, several initiatives exist on a European level to expand the information sharing between the Member States. These include a draft framework decision on the exchange of information under the principle of availability (COM/2005/490) as well as the Prüm Convention signed by 11 Member States outside the framework of the EU.

PRISE will present proposals addressing legal, organizational and technical dimensions and will also discuss what could be regarded as a minimum level of privacy which even in the context of restrictions to safeguard public security must not be infringed.

Among the legal proposals of PRISE are

- the introduction of a mandatory prior checking for security technologies including the evaluation of its efficiency and the level of privacy impact;
- a mandatory evaluation of anti-terrorism laws introducing new investigation powers;
- the introduction of sunset clauses for anti-terrorism laws.

Guiding questions for the workshop to discuss

Directive 1995/46/EC allows for the 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?

In order to introduce privacy awareness and achieve compliance, PRISE advocates the introduction of a Data Protection Management into the research and development process of security technologies. Already at an early point of time of the research process, when defining the functionality of a product, general pri-

vacy principles have to be taken into account. How these principles can be broken down to guidelines for developers will be discussed.

- Regarding the project's main focus PRISE will describe organizational means for the EU funding process to support and consider privacy compliance of research projects applying for funding. These will aim at the three stages of the funding process (application, running project, after release).

Change in political climate – towards a general state of distrust

Participants agree there is a new political climate which leads to legislation assigning new investigation powers and broadening surveillance and collection of information. Every citizen has become a potential suspect in this context. The precautionary principle results in storing data originating form business connections which was formerly not stored other than for billing purposes. This new climate includes a governmental distrust towards citizens and the implementation of security technologies follows this current political climate. A focus of investigations is on linking data from business environments. With respect to this development it is important to consider that privacy friendly features are often not applied by companies as they are considered to cost more. PETs (privacy enhancing technologies) would actually make security cheaper, as a Dutch report showed.

Circumventing national opposition – from the top down

If national governments are faced with too many opposing positions on a national level, a privacy invasive law is introduced 'from the top down', circumventing national criticism by pushing EU legislation on the same subject and then transposing the directive into national law. The European Commission does not stick to its own principles and the privacy level agreed on at a European level as the SWIFT case and the PNR agreement with the US show. In this context it is necessary to strengthen the enforcement of privacy rights. As currently there is a tendency for privacy invasive legislation by the same government that is entrusted with ensuring civil rights, the independent enforcement bodies should be strengthened, that are the European and national Data Protection Supervisors.

Lack of privacy awareness among citizens and stakeholders

A lack of privacy awareness among European citizens can be observed. It was thus regarded necessary to raise awareness and mobilize the citizens as political initiatives which extend existing police laws aim at restoring and fostering a public feeling of security.

But not only citizens, also politicians lack insight knowledge on privacy and PET. It was therefore proposed to issue guidelines for decision makers on privacy and what minimum level of privacy must be regarded when passing laws.

The relation between inner security and privacy

On a more general level, the discussion dealt with the correlation between security and privacy. While one position was that there is no discrepancy between privacy and inner security as both protect the integrity of the citizens, another view was that steps to raise security involve a decrease of privacy. The perspective of whose privacy and whose security is actually addressed has to be clarified when discussing a balance between security and privacy.

Another idea was for PRISE to promote a special level of standardization of privacy in the context of security technology research and development. PRISE will propose the introduction of a Data Protection Management process which will describe a generic approach to ensure privacy compliance in R&D. With regards to standardization it was suggested that one obligation for security research projects funded under FP7 could be to feed into existing standards in their field of research. Also ENISA may help to give privacy supporting input to ongoing standardization by projects such as PRISE or Data Protection Supervisors.

For privacy enhancing security technologies a competitive advantage can be expected as they will make the product more secure. If a privacy seal or audit was introduced on a European level which was followed by a legal obligation for public authorities to prefer audited products over such which are not audited, this would mean a competitive advantage.

Workshop B: Scenarios – Asking the citizens

The development of the implementation scenarios was introduced and there was an introduction to the participatory method that will use the scenarios to introducing security technologies and privacy for lay people in six countries.

The general impression from the discussion is that the participants think the scenarios are good, and that the participatory approach should lead to interesting discussions and results for the project.

List of suggested improvements and comments to the scenarios:

Are the scenarios controversial enough to trigger a discussion?

- Will the lay people read the text? Are the scenarios too long? Perhaps some of the points could be visualized?
- Both the main characters in the scenarios have nothing to hide! There should be a minority person in a more prominent role (there are minority persons in "supporting roles").
- Will this be enough to trigger a discussion? Should there be some more material, e.g. about the dilemmas that are presented implicitly. More focus on privacy problems.
- We are not as intimate as we used to be (20 years ago). We are not so worried. It is more accepted to expose private problems and details in public.
- Information of what telecommunication could do is not very visible in the scenarios
- The description of data retention should focus more on the EU directive.

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?

The scenarios should give a more comprehensive introduction to privacy and the main points in the privacy debate.

- There are some underlying issues and dilemmas in the text – the expert debate about these issues could be described in the text boxes.
- More examples of privacy enhancing security technologies could be given.
- More on the rationales given for installing security measures.

The scenarios should be reviewed to make sure they are not biased

- The scenarios may be a bit biased in the favor of privacy – they should be shown to a few security technology positive persons for comments. (Note: The scenarios have been commented by a group of experts in different fields, among them two representatives from police authorities. The workshop group was later informed of this.)

List of suggestions and comments to the participatory approach:

The results of the interview meeting will depend on the timing and geography

- For the country reports, media documentation from two weeks before and one week before should be collected and presented to show the lay peoples "starting point" in the discussions. This will ensure that the results are viewed in light of recent incidents.

- Geography and culture is also important and must be documented: Is the country a former communist state? Does it have a history of terror? What has the democratic situation been like?

Minority groups should be present at the interview meeting – minorities could be invited separately to make sure that they are represented

- Interest organization for minorities could be contacted (ethnic, sexual orientation etc.).

- It should be considered if the minority representatives should be in one group together, or spread put in the other groups.

- Opinions are very different between different groups of people.

- How good are the respondents in visualizing themselves in the scenario situations.

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?

General discussion on security and privacy

- Security of society is often an argument from the government for invading peoples privacy – is it the security of society or of the people (and their privacy).

- Privacy is a protection of the citizen against abuse of power from the state.

- We should be very careful with putting security and privacy in a "zero sum game".

Questionnaire

- Background questions for citizens – e.g. how do you use your mobile phone?

- Answers do not always coincide with their behavior.
- Questionnaire on these issues – e.g. convenience versus privacy – are difficult. But focusing on the specific examples is not good either.
- The input is very important, because it will affect the answers very much.
- Finding the right level between the big issues and the specific situations.

A draft version of the questionnaire will be sent to the workshop group, so that they can provide input.

Workshop C: Criteria for privacy enhancing security technologies

The introduction to the workshop was a presentation of the PRISE-team of possible ways to workout criteria for privacy enhancing security technologies (see attached slides). After this a fruitful discussion evolved among the workshop members.

Following the main lines of argumentation are listed:

- Definition of security:
  What is needed first is a clear definition of security in the context of the project. This part should clearly discuss whose security against what is meant. What are the different threats to society and the individuals? We need to clarify different security strategies and their efficiency related to specific threats.

- Privacy/security dilemma:
  The discussion showed, that the privacy/security dilemma does not exist in the strong form. It rather seems to be a trade-off between different security aims than one between privacy and security.

- The members were in favour of using existing process-oriented tools of systems design – like the common criteria for IT security – and to enhance these approaches by privacy requirements and monitoring features (see graphic below). A related challenge is how to transfer legal requirements into technology.

- For finding criteria it was stated, that one of the main challenges will be to translate legal requirements into technical solutions.

- Privacy assessment:
  Systems should always be seen in the context of their usage (use and abuse cases). To be able to assess systems against stated criteria it is necessary to know the environment assumptions (who are the legitimate users, whom do you trust, etc.) and to do an overall risk assessment (what could happen to the system?).

Guiding questions for the workshop to discuss

What sets of criteria do exist? What are the criteria for criteria?

What is the privacy-security dilemma all about? What levels of protection do we deal with?

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

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

How would you answer these questions? What is missing?

- Always bear in mind different perspectives of different actors:
  the perspective of the individual is often not the same as the one of the institutional user of security systems (Law enforcement agencies, Ministries, …)

- Demand side important:
  As the security market is mostly a monopolistic structured market from the demand side, it seems essential to raise awareness of privacy issues of institutional (mostly public) customers and to encourage them to stronger demand for privacy enhancing, alternative systems.

- Some basic rules for privacy oriented systems design:

  - Decentred model is more privacy oriented but more expensive to handle in term of IT-security

  - Hard coded systems with clear (single) technical purpose and functionality are easier to design and handle in a privacy enhancing way (misuse is less likely)

  - Access model is important: who can do what? Does the data-subject have any possibility to get access to his/her own data? As part of this, biometric systems may help to ensure privacy friendly access control, but on the other hand may create new privacy problems for users.

  - Basically less efficiency of systems - in the sense of less integration and priority for data minimisation - is privacy enhancing

- Basic recommendations for criteria and evaluation process:

  - There is a need for evidence based security policies

  - There should be different criteria for the whole life cycle of a system (concept, design, implementation)

  - Check lists for systems could help developers to get awareness of the issue

  - A veto for data protection agencies is necessary during the whole process. If the system can be improved the data protection agencies should be able to send it back for refinement.

  - Be aware of existing/developing schemes like privacy standards in the context of ISO/CEN and of research projects, e.g PETTEP (Privacy Enhancing Technology Testing and Evaluation Project; see www.ipc.on.ca) or online tools, e.g. the OECD privacy policy generator.

  - In the context of FP 7 take care of ethics review for proposals. What procedures are in place, what may be used for privacy check? Include questions to be answered by proposers, not only criteria; at the end of the project a complete ethic and privacy review should be provided.

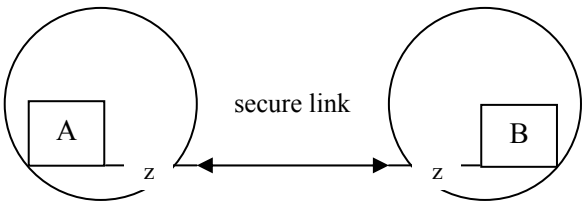
  - Proposers should be encouraged to show privacy enhancing alternatives and provide evidence that no more privacy enhancing alternatives exist.

  - Criteria are not enough – need for measures afterwards

Systems design procedures (enhanced by privacy aspects)

1) Architecture

Privacy and security architecture

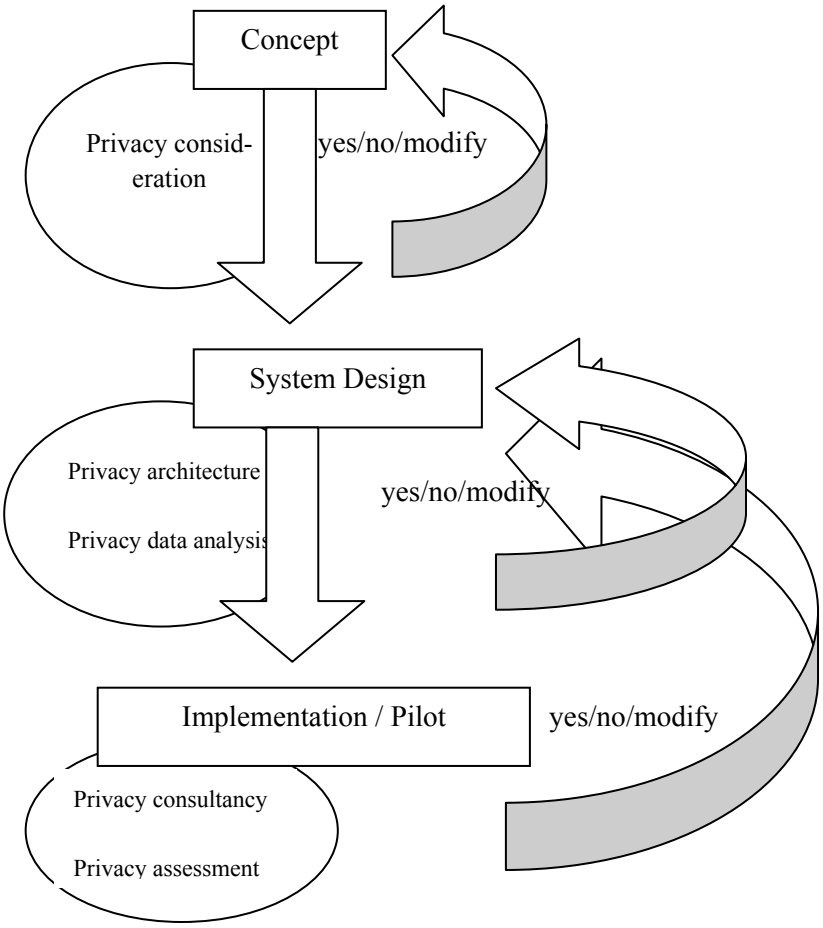


2) Data flow modelling

Where in the system do we have/need what kind of data (systems data, personal data etc.) Does not apply for data mining systems.

3) Use cases

Privacy testing use cases



First brainstorming on possible criteria

Overall recommendations:

- Discuss different security strategy
- Look at the whole life cycle
- Use standard design procedures and add privacy requirements
- Environment and demand side relevant
- Public administration important
- Criteria are not enough – need for some measures afterwards

Criteria for Procurement

- Well defined design process incl. privacy design
- Privacy document
    - Priv-ops cases - (ab)use cases
    - Privacy architecture
    - Show why existing privacy enhancing technologies do not improve design
    - Data access rules/categories
- Test criteria on basis of concrete examples, generalisation as next step
- Security benefit of the system (different approaches and security strategies)
- Means of turning systems off in privacy emergency or in the absence of security benefit
- Means of monitoring security benefit (or lack of it)
- Means of securely destroying data

Criteria for FP7 bids

- Initial Privacy Impact Assessment
    - What privacy information exists in proposed system?
    - Fair Information Principles
        - Can subject see own data?
        - Purpose, consent, notice, access, correction …
    - How is private data held and protected?
    - How long is it stored?
- Privacy objectives and milestones on privacy aspects
- Control of privacy criteria as part of review process

User and Stakeholder Workshop I, Copenhagen

Workshop 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

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) - see the slides from the presentation at http://prise.oeaw.ac.at/workshops.php

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

- see the script for the speech at http://prise.oeaw.ac.at/workshops.php

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

- see the slides from the presentation at http://prise.oeaw.ac.at/workshops.php

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

- see more about the preliminary work in the PRISE-project in the Workshop Paper
http://prise.oeaw.ac.at/workshops.php

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

- see more about the preliminary work in the PRISE-project in the Workshop Paper
http://prise.oeaw.ac.at/workshops.php

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

- see more about the preliminary work in the PRISE-project in the Workshop Paper
http://prise.oeaw.ac.at/workshops.php

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

List of participants

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:

Matthias Schunter		IBM, Suisse
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, Denmark
John Borking	Privacy Adviser	Borking Consultants, 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
Christine Hafskjold	The Norwegian Board of Technology
Åse Kari Haugeto	The Norwegian Board of Technology