PRISE Concluding Conference Statement Paper

Preamble:

Rapid progress in the development of communication technologies, biometrics, sensor technologies and data storage and analysis capabilities is causing constant pressure on the fundamental right to privacy for both economic and security reasons. In addition, the tragedy of 9/11 and subsequent terror attacks have considerably increased the political importance of security and led to the development of new security concepts and strategies that shift the balance between security and the observance of human and fundamental rights. We have seen the development and implementation of new security technologies and measures throughout Europe, which are supposed to raise security for European citizens, but are at the same time increasing the surveillance of citizens and causing infringements of privacy.
A primary task of the PRISE project is to develop criteria and guidelines for security technologies and measures in line with human rights in general and with the protection of privacy. Security technologies that are consistent with and enhance privacy should allow the security industry to develop widely acceptable security products. Integrating privacy in the design of new security technologies and systems will be a competitive advantage for the European security industry. It should be possible to implement them in a way such that in the future more security does not imply a loss of privacy.
The aim of the paper is to state what the PRISE team and the Advisory Panel members think needs to be done to protect privacy in a security-focussed world. It was presented and discussed at the PRISE Concluding Conference.

Why is privacy important?

Privacy is stated as a human right according to the UN Human Rights Convention, the European Convention on Human Rights, the International Covenant on Civil and Political Rights and the Charter of Fundamental Rights of the European Union. The protection of privacy is operationalised in the European Data Protection Directives as well as in the OECD Guidelines on the Protection of Privacy.

Privacy is a prerequisite for democracy, because it shields personal behaviour from state intrusion. Surveillance creates the risk of “mainstreaming behaviour” and thus undermines societal dynamics and democratic traditions.

The dynamics of society is a prerequisite for social development, innovation and economic growth. To act proactively not only with respect to security, but also in taking privacy seriously will be an investment for the future.

Institute of Technology Assessment (ITA), AT
Unabhängiges Landeszentrum für Datenschutz (ULD), DE
Danish Board of Technology (DBT), DK
Norwegian Board of Technology (NBT), NO

How to enhance privacy when developing and implementing security technologies - statements by PRISE:

- **There is a baseline of privacy that is inviolable.**

There is a need to establish a baseline for the protection of privacy, which is inviolable. There may be individual examples that appear to justify serious violations of privacy. However, no one should ever, in the name of security, go beneath a certain baseline in the interference with other people's privacy. Any EU-funded security research project must prove that it provides for sufficient safeguards that it is above this baseline.
To really protect privacy the baseline is only a first step. The PRISE criteria include two additional steps in providing tools for a privacy impact assessment, namely data protection compliance (legal) and context sensitive trade offs (normative).

- **Privacy and security is not a zero sum game.**

There is no linear relationship between privacy and security, it is much more complex. Whereas in some cases more surveillance may increase security, the opposite relationship also exists. More surveillance increases the power of governments, and the abuse of this power is a security risk for citizens. The privacy-security issue is therefore not a zero sum game.
A further unsolved issue is whether security really is improved by certain security technologies and whether a loss of privacy is really required to attain this goal. In arguing that there is always a trade-off between privacy and security there is the risk that the privacy of citizens is no longer given priority and what are assumed to be gains in security lead to accepted losses in privacy.

- **General access for law enforcement authorities to existing databases is not acceptable.**

Minimising data collection and data storage is an important principle of privacy protection. Using vast databases, e.g. from the storing of telecommunications traffic data or Internet behaviour or search engine use, in order to analyse the behaviour of the entire population without specific suspicion reverses the constitutional principle of the presumption of innocence and the principle of proportionality. Privacy-enhancing security technologies and measures must aim at minimising data collection. Access should be based on specific suspicion and require court orders.

- **Preservation of privacy is a shared responsibility.**

If there is the will to do so, the technological and organisational security solutions can be designed to minimize the infringement of privacy. It is however not sufficient to develop

criteria for privacy-compliant security technologies and to produce such solutions. While industry can provide privacy compliant and enhancing technologies, their implementation and in a compliant manner is also a shared responsibility of the entities using these technologies . Privacy protection is therefore the joint responsibility of all stakeholders/entities involved in security technologies and policies.

- **Use of PRISE criteria in FP7 project evaluations is an important step.**

The PRISE project has developed criteria for performing a privacy impact assessment to be used in the FP7 security technology proposal evaluation and other research funding programmes as (part of the) basis for funding decisions. They can therefore be an important safeguard to ensure that public money is only spent on technologies in line with human and fundamental rights and European values. The responsibility of the assessment based on the criteria should be given to special privacy evaluation teams with the relevant (legal, organisational, technical) abilities for the task.

- **Privacy enhancement is an essential non-functional requirement.**

The design of security technologies should aim at avoiding the infringement of privacy. The current practice is often to ignore privacy protection in the design phase or to only offer privacy enhancing features as an add-on. Privacy enhancement should be integrated in systems development. It is possible to develop technologies and implement them without infringing privacy, and this approach should therefore be pursued. Compliance with privacy and data protection laws should become a mandatory non-functional requirement that can be used to judge the general operation or quality of a system; rather than specific behaviours or functional requirements. Provisions should be made to ensure proper and easy auditing of compliance as well as auditing of attempts to circumvent policies.

- **Privacy protection requires continuous further development and reassessment of criteria.**

The criteria are aimed at the FP7 programme but should also be adapted to different contexts. Examples of such adaptations are the evaluation of legalisation or security related regulations, the support of procurement processes or guidelines for the implementation and use of security technologies. There are further reasons that argue in favour of the continuous development and reassessment of guidelines, criteria and privacy impact assessments for privacy compliant security measures and technologies. One is that the range of both the threats and the technical possibilities is permanently changing and evolving and with them the associated infringement of privacy. A second reason is that the effectiveness of certain measures and the resulting violations of privacy may in many cases not be sufficiently determinable in advance. The implementation of security technologies and legal regulations must therefore be reassessed regularly and precautions for the required flexibility to permit the withdrawal of inefficient and infringing measures and technologies should be taken.