PASR

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

Grant Agreement no. 108600
Supporting activity acronym: PRISE

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

Activity type: Supporting Activity

D 5.8 Synthesis Report -
Interview Meetings on Security Technology and Privacy

Revision April 2008

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

Author(s):
Anders Jacobi, The Danish Board of Technology
Mikkel Holst, The Danish Board of Technology

Table of Contents   **page**

Preface

Between May 30th and June 15th 2007, the four partners and two research collaborators[1] of the PRISE project carried out six so-called 'interview meetings' in Austria, Denmark, Germany, Hungary, Norway, and Spain. The interview meeting is a method that combines debate, completing a questionnaire and group discussions. An interview meeting takes three hours and is normally held as an after work event involving 25-35 participants. The six interview meetings of the PRISE project resulted in six national reports[2], which are the basis for this synthesis report. The synthesis report combines the results of the national reports and gives an overview of the participants' attitudes towards new security technology and privacy issues and points out the national differences. The report will occasionally use the terms Hungarians, Norwegians etc. when naming the participant groups from the respective countries, but these only represent the attitudes of the group, not the population.

The synthesis report will start by addressing relevant methodological issues. Chapter 2 is a short introduction to the countries covered in this study, with an emphasis on the different understandings of security and technology that are reflected in the national interview meetings. In chapter 3 the report will briefly go through the attitudes towards specific technologies. Chapter 4 is the main chapter describing the general attitudes towards privacy and new security technologies. It will mainly concentrate on what factors determine the boundaries of privacy and participants' acceptance of security technologies. Finally, in chapter 5 the report looks at democratic issues and presents proposals for privacy enhancing implementation of new security technologies.

The report's main findings are summarised in chapter 6, the conclusions.

---

[1] For Hungary Eszter Bakony from MEDIAN, Opinion and Market Research, Budapest conducted and coordinated the interview meeting, in Spain Vincenco Pavone from Unidad de Políticas Comparadas of Consejo Superior de Investigaciones Científicas, Madrid was the responsible researcher.

[2] The national reports and the corresponding annexes can be downloaded from the PRISE homepage http://prise.oeaw.ac.at/publications.htm.

Executive Summary

This report analyses the results of six so-called interview meetings in six European countries. The results from each meeting have been analysed in six national interview-meeting reports. On the basis of these six national reports, this synthesis report gives an overview of the participants' attitudes towards new security technology and privacy issues and points out some national differences.

Nuanced opinions among participants

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

Acceptability of technologies depended on many factors

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

Concerns about new security technologies

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

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

Public debate needed

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

experts and human rights organisations must be involved to some degree all the way from research to implementation.

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

Basic limits of acceptability
- The threat of terror as such does not justify privacy infringements

- Physically intimate technologies are unacceptable

- Misuse of technology must be prevented

- Function creep is not acceptable

What makes security technologies more acceptable?
- Proportionality between security gain and privacy loss

- Court order

- Strict control

- Privacy infringing security technologies must be the last option

Democratic demands
- Public debate

- Broad involvement

- Always analyse privacy impact

Chapter 1   Methodology

The following paragraphs will briefly address the relevant methodological issues.

1.1   The interview meeting

At an interview meeting a group of 25-35 citizens are asked about their perceptions and preferences in relation to a technology, a technological development, challenge or problem. As a rule, interviewees do not possess any expert or professional knowledge about the technology in question. However, prior to and during the meeting, the participants are informed of the advantages and disadvantages of the technology in order to give them a balanced and factual common starting point. In the PRISE project, this information is based on the scenarios developed in WP4 and the dilemmas these scenarios focus on. The purpose of the scenarios is to make it possible for participants to imagine the consequences of introducing new security technologies into the society. The scenarios can be found in Annex 3.

When making recommendations for research and implementation of new security technologies, it is crucial not only to favour the majority. The validity of the analysis depends on the ability to include diverging opinions and the variety of opinions among citizens. Consequently the interview meeting includes a diverse selection of citizens, selected on the basis of demographic criteria such as age, gender, education and occupation.

Public consultation like the interview meeting is without doubt going to be put to trial on how good it represents the population as whole. But it is important to underline that the purpose of the method is not give a representative answer on citizens opinions. The purpose is to give an indication of what the majority of diverse group of citizens think and feel about a certain technology and more important give a picture of the diverse opinions and the arguments behind them.

1.1.1   The two methods

The interview meeting is based on a combination of two methods, the small-scale survey and the focus group interview. By combining these two methods it is possible to get both qualitative data on the citizens opinions and small-scale quantification of these data.

The Survey

In the survey citizens are asked a number of questions in a written questionnaire. Subsequently the answers of the questions can be summarized in percentages and tables. This gives a picture of what the whole group of participants think and feel about security technologies and privacy and of the variations in the group. When doing a survey it is normal to use a smaller group of selected people, and then generalize the results to a population from which the smaller group was selected. In other words the opinions of a group of selected citizens could be used to generalize on the opinions of the population as a whole. In this report we are very careful not to generalize the results of the interview meeting, as the number of selected citizens is not representative for the population as whole.

The survey is a method based on deductive reasoning. The researcher has to have a pre-structured idea of what to 'look for' and then only has a possibility for getting assumptions verified or falsified by the answers provided. Only little new knowledge is obtained. The

survey is also a very restricted method when dealing with complex issues. Complicated questions are often too open for interpretation by the interviewee or too hard to understand. A questionnaire gives no indication about the reasoning behind the answers, thereby excluding a crucial part of what we look for. Finally, a survey only gives a 'snapshot picture' of the present and does not indicate how public opinion changes through deliberation.

The focus group interview

The focus group interviews counterbalance the limitations of the survey. From the focus groups new and unpredicted knowledge is added to the analysis when the participants speak their mind, reveal their reasons and approach the subject in their own 'language'. The discussions also give the participants a possibility to find a common ground and to develop consensus.

However, if some interviewees are more dominating than others they can influence the debate too much. In addition some opinions and arguments are often found to be more legitimate than others, muting some voices. The questionnaire is a help for us to hear these participants. The questionnaire also aids to structure the outcome of the focus groups by indicating what is important and what are less important to the participants.

1.2   National recruitment and group composition

To ensure reliability, the organisers in the six countries carried out the national interview meetings based on a manual defined in advance that describes the method and gives thorough instruction of how to carry out interview meetings in the context of the PRISE project – the manual can be found in Annex 1. We went great distances to ensure that the methods used were the same in all six countries, as well as the responsible PRISE member was present everywhere.

However, due to national differences, not all the interview meetings were conducted as originally planned.

The Austrian preparations deviated from the interview-meeting manual in the recruitment of participants. The Austrian participants were recruited by phone instead of by mail. Unfortunately, only 17 out of 34 confirmed participants showed up at the meeting. In consequence, only three instead of four group interviews were conducted. The final group of participants was not as diverse as originally intended; it was biased towards older people, people with longer education and women. Collated with the total quantitative data of all participants in the six countries, this should have resulted in a more privacy aware group. However this is unproved conjecture, as some countries have not shown systematically stronger privacy concerns as a result of similar biases.

In Germany as well, the recruitment process was troublesome. After not receiving sufficient feedback on the invitation letters, the German organiser chose to advertise for participants in a local newspaper. At the meeting, the Germans also encountered a high dropout rate. On this background the meeting had no representation of what the German organiser considered to be short education, just as there was an overrepresentation of male participants.

In Spain the organiser arranged four separate meetings rather than one joint event due to Spanish working hours and after work habits. Also the Spanish organiser followed a different recruiting process, arguing that mailed invitations would be regarded as 'spam', whereas advertisements and targeted diffusion of recruitment forms could be more conducive to the

needed feedback. The recruitment was then complemented by phone and the final group was stratified in accordance with the manual. There is no indication that this approach should have biased the findings of the Spanish interview meeting.

The Hungarian organiser also used telephone recruitment instead of letters. The methodology of the random selection of participants and telephone recruitment might prove to have a higher degree of randomness, as the human contact makes it possible to encourage people to participate in the meeting – people who would have been unlikely to reply to a written invitation in any country.

The Norwegian interview meeting followed the interview meeting manual carefully and the participants were recruited as described in the manual. Of the 26 participants who showed up at the meeting, there was a slight overrepresentation of people with long education.

The Danish interview meeting also followed the manual closely. Again, not all invited participants showed up at the meeting, so even though the final group did have the expected composition of age and sex, there was a lack of people with shorter educational background which resulted in an overrepresentation of medium and long educational backgrounds.

Between the countries we find great variation in the proportion of participants with children, both with children living at home and living elsewhere. There is no apparent explanation for this phenomenon, but one could speculate that the demographics vary from city to city and from country to country, just as differences in work and family culture may play a role in who were able to participate.

1.3   Statistical approach

This report will feature several statistics based on the collected data from the meetings. Since the report is not based on a sufficient large number of citizens selected from the participant countries for representative statements, the report will not feature specific numbers and percentages, but rather speak of tendencies. If one wishes to look at the actual statistics, please refer to Annex 5.

The six meetings gathered a total of 158 participants. 51.9 percent of the participants were female, 59.5 percent had children, and 50.6 percent had tertiary education[3]. The median age was 47 years and the average 45.3 years. The participants were distributed as intended between the three age groups and the genders. However, the subset consisting of people with long education was larger than originally intended. The figures on the composition of participants are listed in Annex 2.

The composition does not seem to influence the qualitative results notably, as we find no indications that certain arguments were repressed in the debates. We find the same arguments presented in all the participant countries, which validates the findings. However, the quantitative results could be slightly biased towards a more critical view of security technology and greater awareness of privacy, as this is the general tendency of longer education in the data generated in the interview meeting process.

---

[3]   ISCED-97 level 5 & 6.

We seek to avoid drawing conclusions that do not have general relevance, by not making references to specific statistical figures. Instead we will only speak of rough shares and broad tendencies.

1.3.1   Statistical results compared

Finally even though this report does not claim to present representative results we would like to address the question of how good the results are as an indication of the public opinion by comparing the findings in this report to findings from representative statistical research on the same subject. It appears that only little quantitative work has been done on privacy issues. On top of this it has been necessary to disregard most existing surveys done on this subject, as approaches, questions and wording diverges from the ones used in PRISE, making comparison practically impossible. The questions used here for comparison are chosen on the grounds of comparability. From the available research we compare the results of PRISE to questions from Special Eurobarometer 267 and a survey done by the Norwegian Board of Technology based on the PRISE questionnaire.

We conclude that in general the statistical results from the PRISE meetings seems as good indications of the general attitudes found in Europe, as long as they are treated as rough indications.

Special Eurobarometer 267

Special Eurobarometer 267 "Use of Intelligent Systems in Vehicles"[4] approaches the question of privacy intrusion by instalment of the 'eCall' system in vehicles, which is also approached in the PRISE questionnaire.

In the Eurobarometer survey, the interviewees are asked if they regard eCall to be a privacy intrusion[5]. In the Eurobarometer 82 % of the citizens in the 25 EU member states would accept eCall to be installed and used for accident reporting[6] (disregarding 'don't know' answers). In PRISE 78 % would accept this. However, when we compare the national results, we find greater divergence, especially the Danish PRISE group appears more privacy aware than the Danes in Eurobarometer.

Even though we have to take into account differences of wording and approach, this in general validates the findings of PRISE as a useful indication of the general attitudes in Europe. However, we should be careful not to draw too strict conclusions on the national differences.

---

[4] Report can be located at http://www.ec.europa.eu/public_opinion/archives/ebs/ebs_267_en.pdf (April 2008)

[5] Half of the respondents were asked the question "Cars can be equipped with an emergency call system which automatically calls the local emergency authorities when the vehicle is involved in a serious accident. This system instantly transfers to them accurate vehicle position and other accident related data and thereby reduces the time for the rescue services to arrive. Some people might consider this system as an intrusion on driver's privacy. Do you personally regard this as…?" and half "Cars can be equipped with an in-built system collecting information such as their location or speed, in order to produce real time traffic information. Some people might consider this system as an intrusion on driver's privacy. Do you personally regard this as…?".

[6] Answers "You do not consider it as an inconvenience as far as you are concerned" & and "A minor inconvenience compared with the usefulness of the system".

NBT PRISE Survey

The survey done by NBT measures general attitudes towards new security technology in Norway based on the PRISE questionnaire[7]. However, in the survey many of the questions differ from the original questionnaire, making them unsuitable for comparison. The most suitable question approaches the discomfort connected to surveillance. We find that roughly 57 % of the Norwegians find it uncomfortable to be under surveillance and 31 % do not[8]. In the Norwegian PRISE meeting the shares were 65 % and 23 %.

This suggests that the Norwegian participants are slightly more privacy aware than the population in total. But again, if the results are considered as rough indications there seems to be conformity between the PRISE results and results of representative surveys.

---

[7] More on the Survey can be found at http://www.teknologiradet.no/FullStory.aspx?m=28&amid=3673 (Norwegian) (April 2008)

[8] Question 20 in the PRISE questionnaire.

Chapter 2   Overview of National Differences

When reading the national reports, it is evident that the participants from the six countries have different basic understandings and perceptions of the terms security and privacy. Differences in perception of threats, differences in trust in others and in institutions and differences in perception of privacy are shaped by history, media attention, recent incidents and debates. The basic understandings serve as an influential backdrop of common references and established norms that shape the debate.

2.1   Spain

Spain has a long history of terrorist attacks from the ETA organisation and only a few days before the interview meetings ETA ended their 'temporary ceasefire'. Furthermore, the interview meting was held in Madrid where in 2004 there was a serious terrorist attack with bombs on a number of trains. On that background the Spanish participants could be expected to be especially aware of the threat of terror and the need for security. This does not seem to be the case. Instead the Spanish report more than once emphasises that the most important issues for the participants were gender violence and sexual harassment. Many of the security technologies were debated in light of this. The report also emphasises a big mistrust in official institutions and commercial interests, which in general leads to mistrust in new security technologies. As others, the Spanish participants mistrust the people in direct control of the technologies. They do not, however, only focus on misuse, but also on human errors. Finally, it should be noted that more than half of the participants changed their attitude at the meeting, some became more privacy aware and some became more positive towards security technologies.

2.2   Hungary

In Hungary as well, there was a great change in participants' attitudes because of the meeting. Here the participants clearly called for more information and more debate – some expressed a feeling of lack of education in schools and some called for TV-programmes that deal with the issues. Even more explicitly than in Spain, the Hungarian participants expressed mistrust in official institutions. General mistrust exploded last autumn when a leaked recording of the prime minister admitting lying and accusing fellow politicians of the same was followed by public uprising. After several incidents of misuse of power the police struggles with a bad image. The debate over public moral, or lack thereof, seemed to influence the perspectives on the need for security technologies – the Hungarian participants called for a change in morality over implementing technological solutions to security problems and some argued that new security technologies might even help improve the social moral. On top of that, the Hungarian meeting, as the only one, also expressed hope for a national security industry and that this could attract capital to the country.

2.3   Norway

The Norwegian participants expressed little fear of terrorist attacks. They accordingly dealt with security technologies in the light of other forms of crime. The frame of the meeting was also affected by earlier public discussion over the Internet phenomenon 'Facebook' – a social networking website where users voluntarily share personal information. Consequentially, data retention was discussed a lot and the major part of the participants was critical towards commercial interests and their willingness and possibility to infringe on the privacy of citizens.

In addition the Norwegian participants appeared to be more critical towards locating technologies than any other group. At the same time the Norwegians only had little debate on camera surveillance, which too distinguishes them from the other countries. Finally, the Norwegian group showed a very high degree of trust in their official institutions.

2.4   Germany

In Germany much of the meeting has apparently been framed by an on-going debate on the juridical consequences of new security technologies more than in other countries. Germany has a long history of discussions over data-retention that has resulted in strict legislation in this area. Germany is also considered to be one of the European countries with the highest protection of privacy. The German participants take the most critical view on collection of data with or without suspicion of criminal intent. Measures not based on a concrete suspicion, just like the measures used by very intrusive security technologies, are only accepted if based on a court order.

2.5   Denmark

The Danish report suggests a general trust in the public institutions, and compared to some of the other countries Danes only agitate for mistrust on an institutional level to a lesser extent. At the same time Denmark has not experienced a serious terrorist attack, so even though Denmark is exposed due to the cartoon crises and participation in the conflicts in Iraq and Afghanistan, the Danish participants might be more critical of the need and effect of new security technologies, very much like the Norwegian participants. However, contrary to the Norwegians, the most debated issue was that of camera surveillance which appears to be the symbol of new security technologies in the Danish debate.

2.6   Austria

In general, the Austrian participants did not believe that security technologies can completely eliminate risks of crime or terrorism. The current level of attention to threats of crime or terrorism was itself regarded as a potential threat to freedom and privacy as it may cause people to accept violations of privacy and civil freedoms that otherwise would be rejected. The democratically legitimised bodies should basically take responsibility, although there was some doubt to what extent they are acting in the public interest without being too much influenced by external economic and political interests. Hence public information and debate as well as the involvement of independent experts in decision-making is demanded. Some Austrian participants were however concerned about the possibilities to find independent experts or to reach consensus among citizens. The Austrian participants were generally very privacy aware and sceptical towards the need for new technologies, and they argued for other solutions to problems of crime or terrorism.

Chapter 3   Perceptions and Acceptance of Specific Security Technologies

This chapter will present the attitudes towards different groups of technologies. The technologies are biometrics, camera surveillance (CCTV), scanning technologies, locating technologies, eavesdropping, data retention and privacy enhancing technologies.

Obviously the different technologies received different amounts of attention from the participants and there are national differences as well. People have stronger feelings – positive and negative – about technologies they are familiar with and technologies with iconic status in the respective countries, e.g. CCTV in Denmark and Facebook in Norway (see Chapter 2). More complex technologies are usually treated with greater scepticism.

3.1   Biometrics

A considerable minority of the participants did not accept facial recognition, fingerprints or iris recognition under any circumstance. For those who might accept some form of biometric access control, fingerprints are the easiest to accept, iris recognition second and recognition of facial characteristics the least accepted. Only in airports and at borders would a majority accept biometric control – a considerable group would accept to be pre-registered to have easier access control in airports, but not in other public transport. This was especially true for people who travel by airplane at least once a year. The main concerns were identity theft and function creep. Central registration of biometric data was especially not popular. The Norwegian group was the most positive towards these ideas and the German group was the most negative, reflecting the different basic understandings of security and privacy among the participants in these two countries.

3.2   Camera surveillance

One of the most debated technologies was CCTV. Notably the Hungarian representatives were very positive towards this form of surveillance, whilst the Danes were deeply divided and spent much time discussing it. A majority of the participants welcomed CCTV in most places, but CCTV in all public spaces and in intimate situations was deemed too privacy infringing. Active camera surveillance could only gain some support, if it was ensured that no false positives would occur and it was only implemented in exposed places. There was no clear indication whether there was general wish for more CCTV – especially the Norwegians found it hard to consider this question, which was also reflected in a general lack of debate on CCTV at the Norwegian meeting. While there was a shared perception of CCTV as a good tool in police investigation, there was a call for more knowledge on the actual effectiveness of CCTV. Lack of effect was one of main arguments for the need for research in alternative solutions.

3.3   Scanning technologies

Acceptance of scanning seems to be connected to sites of use, as it was widely accepted in airports, but nowhere else. Commonly encountered scanning technologies such as scanning for metal objects and x-raying of luggage are widely accepted, but newer methods like full body scan *without* projection and scanning of sweat, body heat and heart rate are not well received. Full body scan *with* projection on a virtual mannequin got highly different responses in

different countries – the Hungarian group was by far the most positive, while the Spanish and the Austrian were the most critical.

3.4   Locating technologies

Even though the participants widely agreed to the claimed potential of locating mobile phones and cars for crime prevention and investigation, a large majority of the participants would only accept the use of these technologies based on a court order. The reason is the feeling of privacy intrusion that these technologies generate – the juridical institutions can to some extent contain this negative effect.

eCall turned out to be an especially interesting technology, as it raised a series of relevant discussions: If the majority of the participants should accept eCall, its installation has to be voluntary. This accentuates a dilemma in the choice between optional security technologies and their effectiveness – as long as eCall is optional, its effect will of course be limited. Frequent motorists were more likely to support automatic installation of eCall.

The attitude towards eCall was completely different when the intended use was presented as use in case of emergencies – then a majority supported the use of eCall. The intended use of the technology, not the technology itself, determines a substantial part of the accepted privacy impact. The participants were very reluctant towards automatic fining of speeding, and a little more positive towards using eCall to locate stolen vehicles. This emphasises the importance of defining not only the general use, but also what specific crimes the technology is supposed to target.

Interestingly, the Norwegians were more critical towards any form of locating technology – the idea of being located seemed to be in greater conflict with the Norwegian participants' concept of privacy.

The Spanish participants were very keen on using location technologies for private surveillance of children and the elderly. This use of the technology was not widely accepted by participants at the five other interview meetings.

3.5   Eavesdropping

As with locating technologies, acceptance of eavesdropping depended on the police obtaining a court order. Even though it was broadly recognised that eavesdropping was a good tool in police work, collectively the participants could only accept eavesdropping on a suspect, not on his or her expected contacts and even less on all communication lines. Again this is closely connected to the feeling of privacy intrusion created by the technologies. The feeling of intrusion was most widespread in Germany and least in Denmark – probably as a result of the traditional trust in governmental institutions.

3.6   Data retention and data mining

A majority of the participants accepts retention of data for specific purposes. Also a majority can accept scanning of data and combination and analysis of data, but only if it is used for investigation of crime and terror. A significantly smaller part of the participants supports preventive use, although the Spanish participants and to lesser extent the Hungarians and Norwegians are supportive of this form of use.

In general, it is accepted that data retention as well as scanning and analyzing data are good tools for the police, but this conflicts with a strong feeling of privacy intrusion and a strong fear of function creep initiated by institutions or individuals. As a result about 1 out of 7 participants would never accept data retention, if they were to choose – more in Germany and less in Spain.

Data retention by government institutions gains more support – the participants were slightly more positive than negative towards this. The most positive countries were Denmark, Norway and Spain.

3.7   Privacy enhancing technologies

The participants seemed to be very unsure about privacy enhancing technologies (PETs). The technologies and especially their consequences appeared to be hard to comprehend for many. This is probably due to lack of knowledge about these technologies. This could also explain the fact that PETs were not discussed much at any of the six interview meetings.

In general, the participants argued that PETs were much needed to preserve privacy. However, when the discussion touched upon actual technologies and specific consequences, the support dwindled. Slightly more than half the participants accepted use of encryption and slightly less than half accepted the use of anonymous calling cards and identity management. When it was pointed out that some technologies could prevent investigation of specific crimes such as distribution of child pornography, they gained even less acceptance. A small group would never accept PETs under any circumstances, if it conflicted with police work.

Generally, PETs had more support in Austria and Germany than in the rest of the participating countries.

Chapter 4   Participants' Attitudes towards Privacy and Security

Not surprisingly there was a clear overall connection between the level of privacy infringement caused by a technology and the level of acceptance of the same technology. At the same time the six interview meetings revealed that the level of acceptance was determined by a number of other factors, e.g. familiarity, site, situation, effectiveness of the technology, all of which should be taken into consideration when developing and implementing new security technologies. The specifics of these observations will be described in this chapter.

4.1   Nuanced attitudes among participants

It is important to emphasise that the participants at the six interview meetings in the six different countries had a broad variety of opinions and some highly nuanced attitudes towards privacy and security. The participants showed great insight as well as willingness to discuss, argue for their opinions and listen to and learn from the opinions of others. Often the participants were confronted with dilemmas that challenged their overall opinion and revealed their willingness to compromise their attitudes. And depending on the circumstances, a majority of the participants are willing to relinquish some of their privacy in specific situations.

4.2   General attitudes and positions

Still there are tendencies that allow dividing the participants into three main groups. Based on the answers to questions about general attitude towards privacy and security[9] and the analysis in the national reports the groups can be divided as follows:

- The biggest group is the participants that weigh privacy as an important right and are worried about the use of security technologies and the infringement of their privacy. This group consists of roughly 60-70 percent of the participants.

- The second group is the participants who do not perceive surveillance and security measures as something unpleasant and believe their implementation will result in a considerable gain in security. This group consists of roughly 20-30 percent of the participants.

- And finally there is a group of undecided participants who do not perceive privacy infringement as a substantial problem in their lives but still do not support extensive surveillance measures or use of security technologies. This group also finds that the security-privacy dilemma is very complex and difficult. Approximately 10 percent of the participants belong to this group.

It is important to emphasise that these are rough categories that do not grasp the complexity and variations of the participants' opinions and attitudes. These will be elaborated in the following.

---

[9] Question 15 - 20 in the questionnaire, see questionnaire in annex 4 and frequency tables in annex 5

4.2.1   Are security technologies necessary?

The question of whether the security of society is dependent on the development and use of security technologies divide the participants. Just over half the participants agree that our security is dependent on technology. Likewise, Just over half the participants agree that when security technology is available we might as well make use of it. The technology-positive participants commented:

> *"I tend to think that whatever fosters security is okay with me. This is why I do not understand some of the debate; why do people worry if there are so much bigger dangers for mankind than giving away your data." (DE)*

On the other hand, a number of participants do not consider technologies to be the right way to protect oneself against crime and terror. They stress that it is more a social problem than a technical problem and that the solution should also be social rather than technical. Especially the Hungarian participants emphasised this in their group discussions.

> *"The causes that generate terrorism should be abolished." (HU)*

> *"It is a thought of mine during the discussion, all the governments should not be fixed to the idea that we need new security technologies, because we have to fight crime and terrorism. Maybe one should go back one step and fight against what is the real problem, one cannot solve terrorism with x-ray and scanning alone." (AT)*

They point to education, integration and better economic conditions as means to prevent crime and terror.

Many participants across the six countries emphasised that it is far more important and far more effective to look at the causes of crime and terrorism than to implement security technologies as protection against terror:

> *"I would say in relation to security technologies that the social climate or atmosphere should be improved first, and it would be much more effective and secure – if we take this word seriously – than to set up the technology. If fewer people have the feeling that they have nothing to lose, then less people should be kept in check." (HU)*

Interestingly, the participants were very positive towards the technologies, if their purpose was to prevent or help out in case of accidents. This indicates that the feeling of privacy infringement is strongly connected to the feeling of being under suspicion, not to the actual technology.

4.2.2   Violation of privacy

Overall, a vast majority of the participants feels that privacy should not be violated. 85 percent of all participants agree that privacy should not be violated without reasonable suspicion of criminal intent. The participants are aware that security technologies will violate privacy to some extent. A vast majority (80 percent) also feels that it is unpleasant to be under surveillance. These numbers indicate that participants in general weigh privacy higher than security, but the group discussions reveal a much more nuanced attitude towards the balance of security and privacy.

> *"Still, I consider privacy to be a high value and that it may prevail public security. Not every information that can be collected should be collected." (DE)*

> *"Privacy has to do with my free will, with my free decision. In the moment when I give up a part of my privacy, I also give up part of my decision, of my will; (…) then I prefer more risk." (AT)*

Privacy infringing security technologies are indeed accepted in some places and situations. What causes disagreement among the participants is when, where and how much violation of privacy they can accept. The participants' have very diverse limits and attitudes towards this:

> *"We have to restrict our freedom in some degree to have security." (HU)*

> *"I'm sitting here as a law-abiding citizen. It is easy for me to say: Just register it all, no problem in that. But the problem is that you can imagine the situation where registration could become a problem even though it is not in connection with anything criminal." (DK)*

Some participants also point out that the perception of what violation of privacy is could vary from individual to individual.

> *"(…) people participate voluntarily in "Big Brother". It is a tendency in the society that it seems that people don't think it is that important having a private sphere anymore" (NO)*

The group debate in Spain stressed the opposing sides via this rhetorical question:

> *"If I have nothing to hide, why should I worry?" (ES)*

And the opposite question:

> *"If I have nothing to hide, why should they monitor me?" (ES)*

In general, a majority of the participants seems to prioritise privacy high, but even for this majority there are definitely situations and places where security is more important. This will be elaborated below.

4.2.3   The perception of danger

A crucial part of the discussion on security technologies concerns the definition of what one seeks to be protected from. What characterises the danger? How big is this threat? Some participants came up with some interesting answers:

> *"The biggest problem in Norway today is traffic accidents and heart attacks" (NO)*

> *"Executives were talking about the danger of terrorism, because it was their interest, but it's terribly destructive. Because a lot of people are really afraid. Presently, Hungary doesn't really have to be afraid of terrorism." (HU)*

However, most of the participants in the six countries did see the threat of crime and terror as big enough to justify some security measures and technologies. The question, then, is what

kind of crime and terror can justify security measures and violation of privacy. The participants often distinguish between terror, serious crime and petty crime and there is no doubt that while terror and serious crime for most participants can justify some privacy infringement, petty crime, e.g. speeding and shoplifting, cannot.

In Spain, the participants pointed to gender violence and other 'serious crime' as the most legitimate targets of security technologies, while the Austrian participants find neighbourhood protection more important than protection against terrorism. In most countries criminals were considered as a bigger threat than terrorists. In Norway, Denmark, Austria and Hungary terrorist attacks were not considered a big threat.

4.3   Taking effectiveness into consideration

The effectiveness of security technologies has decisive influence on the degree of acceptance the technology receives among the participants. The effect of security technologies must be in proportion with the privacy infringements.

The participants question the effectiveness of security technologies. Approximately 70 percent of the participants in the six countries completely or partly agree to the statement that many security technologies do not really increase security, but are only being applied to show that something is being done to fight terror. The technologies are simply implemented for political reasons.

> *"For instance this data retention (...) the guy who crashed with the plane (reference to the 9/11) (...) what was contained in his database? That he had studied as an aviator? And so what? This is not dangerous, they can get around it and this is why I think this technology doesn't lead anywhere." (ES)*

Especially the promise of prevention of terrorism fosters scepticism among the participants. On the other hand, there is widespread belief in the investigative effect of security technologies, e.g. CCTV. So while the participants do not think technologies will be able to prevent terrorism, many participants find the technologies to be a good tool in the investigation of terror and crime.

> *"The problem is that even if you put up more and more cameras you will not have enough personnel to watch them all, and people know that. So I think it is a kind of pseudo-security." (DE)*

> *Yes, but it gives the opportunity to determine the perpetrator afterwards, even if you cannot prevent the crime." (DE)*

When it comes to the effect on crime, some participants argue that the technologies have no effect on crime or just move it to a different area. They argue that security technologies only give false security:

> *"I actually think it gives a high degree of false security. I think it is really a bit worrying. It's a little bit to please the old ladies (…)" (DK)*

> *"(…) crime rates are decreasing where surveillance cameras are deployed, the problem however is, that the whole thing is moving somewhere else…" (AT)*

At the same time, however, to many participants ordinary crime seems to be a greater cause for concern than terror. The Spanish participants were much worried about domestic violence, and the possibility of preventing it by using security technologies – e.g. CCTV – was debated in the Spanish group discussions.

A minority of the participants showed more faith in the effectiveness of the technologies and found that the technologies make them feel more secure. At the group interviews in all six countries there were participants who expressed belief in the preventive effect of security technologies, especially on crimes like violence and theft.

> *"I'm surprised that you assume that there is mistrust towards the surveillance society. I'm very surprised. I feel very comfortable, if there is surveillance." (DK)*

> *"Personally I want it to be a lot of surveillance! (…) I really can't understand why people fear to be monitored in their own country if they didn't do anything wrong." (NO)*

Overall, the group discussions in all of the six countries reveal that the effectiveness of the technologies is a key factor. Technologies that are considered effective in preventing crime and terror have much higher degree of acceptance. Some participants even suggested speeding up the research process in order to develop better and more effective security technologies.

4.4   Security technology is more accepted in 'danger spots'

Some situations and places are considered more suitable for implementation of new security technologies. One possible reason for this is that these situations and places are considered more vulnerable and exposed when it comes to crime and terror.

> *"There are places, dark places, where I would say that it feels good to see a camera at use there; whether it is turned on or not, I don't know, but at some places it can facilitate a feeling of security." (DE)*

> *"I am very ambivalent in these affairs. On the one hand, I have the impression they deploy it excessively, on the other hand, at specific places (…) I consider it as justified." (AT)*

The best examples of 'danger spots' are probably airports. It is illustrative that 90 percent of the participants can accept CCTV surveillance in airports. Also banks, stations and sports arenas are places where more than half the participants can accept CCTV, while in the other end dressing rooms are places where surveillance is unacceptable to the vast majority.

In these "danger spots" security technologies, such as scanning and surveillance, are often already implemented. Consequently, the participants are familiar with security technologies in these situations.

4.5   Acceptance is dependent on convenience

Not surprisingly, the acceptance of security technology depends on the feeling of loss or gain of convenience. Technologies that are imagined to be very inconvenient are not as accepted:

> *"It would have enormous consequences if you were to security check all passengers going to work and changing trains at the main station." (DK)*

On the other hand, this also means that security technologies that hold the potential for a high gain of convenience can be accepted to a higher degree. This support, however, is mainly found among people who are generally not sceptical towards security technologies or have more convenience to gain, since they may interact with the technology on a regular basis.

4.6   Little acceptance of physically intimate technologies

There are signs of some 'natural' barriers to privacy. When the naked machine is considered to be unacceptable by the majority of participants, when iris recognition is preferred over facial recognition and when data mining encounters a high degree of resistance, the apparent conclusion is that the personal space is violated, even though the technology is considered effective and the handling trustworthy. Technologies that target the body and are able to recreate a recognisable identity provoke feelings of intrusion, which is not the case when security technologies only have a public gaze, as CCTV.

The participants expressed it tersely and clearly:

> *"Not inside my intimate sphere!" (DK)*

> *"In addition, to transilluminate, to go through the body, this is also ethically very dubious." (AT)*

One participant had experienced the naked machine and said:

> *"You did really not feel comfortable by passing through" (NO)*

It is notable that the concept of intimacy can vary from individual to individual – and between countries – even though it cannot be analysed from the data from the interview meetings. It is also worth noticing that some technologies are considered less invasive even though they are actually much more invasive. This goes for iris recognition that is seemingly not considered to be as privacy infringing as facial recognition. This can be explained by necessarily missing detailed explanations in the background materials and the resulting lack of knowledge about a technology such as iris recognition.

4.7   Irreversibility of implemented security technologies

Hungarian and Danish participants emphasised that if a security technology has been developed, it is there to stay and at some point it will also be taken into use – and perhaps not the way it was intended. One participant compares it to the atomic bomb:

> *"It is like preventing the a-bomb. Once it has been invented it is very difficult to keep preventing it. Some day it will show up in a place where it wasn't supposed to be." (DK)*

> *"We should not imagine that even if in the course of time a specific security technology turns out to be ineffective or not necessary, that this measure or technology will be revoked." (DE)*

The irreversibility of the technologies suggests that implementing new technologies should be based on extensive consideration.

4.8   Security technologies will be abused

There is a strong conviction among the participants in all of the six countries that new security technologies will be abused. In Spain for example, the participants explicitly expressed their concern that security technologies can be used for commercial purposes or political control.

> *"Definitely. Abuse is written in big letters above it. Above each advantage." (AT)*

4.8.1   Mistrust in institutions

More than 60 percent of the participants in the six countries believe that new security technologies are likely to be abused by governmental agencies and almost 90 percent believe that criminals will abuse them. Especially Hungarian participants are sceptical towards governmental institutions and expect misuse from the state. This could be understood on the background of the former socialist regime in Hungary where citizens' privacy rights were infringed considerably.

> *"These systems, here in Hungary, don't work the way as they should work." (HU)*

The biggest concern for the participants seems to be that commercial interests will misuse information and data collected via security technologies.

> *"All technology can be misused anyway. So there will be persons that try to exploit this." (NO)*

> *"Private companies, I think they can be interested in biometrics in order to know consumption habits." (ES)*

4.8.2   Fear of function creep

The fear of misuse is often a fear of 'function creep' – that the technologies or data will be used for other purposes than originally intended. In this way there is a close connection between the feeling of privacy intrusion and the trust in the institutions that control the security technologies.

> *"What really bothers me about these monster-databases is that the data can be used for other purposes, which have nothing to do with the initial purpose." (DE)*

> *"These technologies should not be used for purposes different from those that are officially established, that is the security of all the citizens" (ES)*

Advanced security technologies often hold the risk/possibility of function creep.

4.8.3   Control of the operators of surveillance technologies is crucial

One thing that many participants across the six countries find problematic is the control of access to these technologies. There is a widespread concern among the participants about who has access to information and data from security technologies and about potential abuses of access to generated and collected information.

"There is just this one snag in it, that there are people sitting on the other side of the technology controlling it. And everybody knows what happens to people when they get power. Power corrupts!" (DK)

Especially Danish and German participants are concerned about the insight given to individuals who have access to data collected from security technologies. But also the Norwegian and Spanish participants mentioned this consideration.

"Whenever humans are operating systems or if someone can gain personal advantage, you have to expect misuse." (DE)

"Then as far as possible you have to guard against misuse. Individuals should have as little power in the system as possible." (DK)

"I don't mind collection of data. But what happens to them, and who get access to them is the most important question." (NO)

"I believe that they should be careful about who is going to have access to our data, to all our data, to all our private things." (ES)

The Spanish participants also expressed anxiety about the competence of the people controlling the technologies

"I don't know how many of these CCTV cameras are attended by security guards, which is a job like many others. I mean, it does not entail special requirements. I mean, if you spend your time monitoring people and you have to decide whether any person is showing ´strange´ behaviour, you really need to have some knowledge about peoples' attitudes." (ES)

In Hungary there seemed to be a more widespread mistrust towards the governmental institutions in general, including the bureaucrats.

However, many participants believed that with proper control exercised by competent authorities security technologies may indeed improve the level of security in given areas of people's lives. The Norwegian participants revealed a high degree of trust in the state.

4.8.4   Court orders make a difference

Some security technologies have a built-in conflict. The vast majority of the participants consider them both a good tool for police in prevention and investigation of crime and terror and at the same time they find them to be very privacy infringing. This goes especially for eavesdropping and location technologies and to some extent also access to collected personal data. For the use of these technologies the participants stress the importance of a court order:

"It makes a huge difference if the police, no matter what they do to me, if they get a court order first. Then it might be that sometimes there is a judge saying yes to everything, but anyway it has been by a judge, and then I can feel the tripartition of power and then I feel more comfortable." (DK)

In general, the questionnaire reveals that approximately 80 percent finds police use of privacy-infringing technologies acceptable, if it is based on a court order, while only about 10 percent can accept them without a court order.

4.9   Private surveillance

At many of the six interview meetings private surveillance was stressed as something particularly interesting – but for different reasons. Danish participants felt offended by the possibility of private surveillance, even though private surveillance of children or the elderly could help to protect them. Also Hungarian and Austrian participants opposed surveillance by private persons.

At the Spanish interview meeting the participants took the opposite position: That surveillance technologies could be helpful especially in relation to taking care of children but also the elderly. Additionally, they argued that private surveillance could help to prevent and investigate theft and gender violence. Some suggested installing CCTV at main entrance doors.

Chapter 5   Views on Democracy and Regulation

5.1   Democracy and participation

The participants in the interview meetings in the six countries were also debriefed about democratic issues concerning the development and implementation of new security technologies.

5.1.1   Involve the citizens in important questions

Continuous public information and transparency concerning the reasoning behind and consequences of implementation of new security technologies is crucial to the public legitimisation of these technologies. 90 percent of the participants across the six countries demand that politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies, whereas only a small minority finds issues of security and privacy to be too complicated to include the general public.

Some participants argue that the people who are going to live with the technology must be heard before the technology is implemented:

> *"Because if things go wrong these are the people who are going to suffer from their consequences, both negative and positive ones." (ES)*

The small minority who did not think the general public should be involved in decisions about security and privacy argued:

> *"(…) I believe that the ordinary citizens... that we would never reach consensus on these measures, never." (ES)*

Because of the high dropout rate, the registered participants for the Austrian meeting that did not show up were asked why afterwards. It is mentionable that some of them stated that they felt the issues at stake were too complex for them to participate in the discussion.

5.1.2   Let politicians decide after public debate

The group debate revealed that most participants across the six countries argued for an open debate, information and a transparent decision making process in which politicians listen to the voice of the public. In Germany and Denmark the participants argued for leaving the decision making to the politicians once the public opinion has been heard:

> *"After a broad public debate it would be reasonable if the politicians made the decisions. That is our democracy." (DK)*

> *"Politicians will represent the opinion of the public." (DE)*

The Norwegian participants also emphasised the need for involvement of the public on other grounds than pragmatic ones:

> *"This is not only something to understand, this is about values." (NO)*

Overall, the participants demanded for public involvement and transparent decision-making.

5.1.3   Demands for the decision-making process

More than 90 percent of the participants believe that human rights organisations are always entitled to be heard when important decisions on security and privacy are made. The participants see human rights organisations as spokesmen for individual privacy.

It is also remarkable that not a single participant in all six countries disagreed with the statement that it is imperative to elucidate and include alternative solutions in the debate as part of the decision making process. This indicates that the participants prefer non-technological solutions instead of implementation of security technologies if possible. As one participant puts it:

> *"If you had two policemen patrolling, going around whistling, right. That would be ten times more effective than a video camera." (DK)*

The participants were more divided about whether to include private producers of security technologies in the decision-making process. Little more than half the participants across the six countries thinks that security industry should be involved because of their expert knowledge, but many were more critical towards the involvement of private producers of security technologies:

> *"One must not forget that there is an economic lobby behind the whole thing." (AT)*

On the other hand, there was broad consensus on involving experts in the debate and taking decisions on a background of scientific analysis.

> *"I think it is important to include experts. Citizens cannot follow what it is all about." (DE)*

> *"Scientists who can explain it well, understandably for the average people. Not the politicians … People should be also asked, but it's impossible to ask everybody. But they must be informed." (HU)*

> *"The experts have to be listened to and it should be taken into consideration what they confirmedly say." (HU)*

5.2   Proposals for privacy enhancing use of security technology

At the end of the questionnaire the participants were asked to evaluate the importance of four proposals for privacy enhancing use of security technologies. In general, the participants found all of the four proposals to be important. The proposals were evaluated as shown in the following table.

Proposal	High import.	Some import.	Little import.	Not import.	Don't know
Collection of personal data from unsuspicious individuals must be anonymous until identification is authorised by court order	127	19	5	3	4
Only authorized personnel shall have access to collected personal data	148	9	0	0	1
Prior to implementing, new security technologies must be checked for privacy impact	127	26	2	0	3
Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts	100	31	13	5	9

The proposal that was evaluated, as being most important by the participants was that only authorised personnel should have access to collected data. This proposal meets the concerns that many participants expressed about the individuals behind the technology and the personal information these individuals will be handling. The Spanish participants also emphasised the need for improving the morality of these individuals.

The two proposals about anonymous data and the proposal about a privacy check before implementation were both evaluated as important as well, while the last proposal about research funding was evaluated as slightly less important than the other three proposals. In the Danish group interview, though, the possibility of regulating the development was mentioned:

> *"Like you try to regulate companies, e.g. no pollution (…) In the same way it must be possible to make some demands to companies developing security technologies." (DK)*

Aside from the proposals with which the participants were confronted, they themselves made some proposals on how to enhance privacy in the use of security technologies.

5.3   Develop alternative solutions

The Hungarian participants emphasised the need to add focus on the causes of terror and to fight them by means of education, integration and social equality instead of implementing security technologies.

Both in Denmark and Austria the participants suggest having more security personnel, e.g. more policemen, instead of implementing security technologies.

> *"I believe it would be better, if police forces were present, who could prevent an attack from the outset." (AT)*

5.4   The dilemma of optional use of technology

Through the meetings it became clear that in all countries a certain minority was not willing to be subjected to new security technologies, especially if they had a choice. There will also be a small group of people who are not capable of using the technologies; this could be workers whose fingerprints can no longer be read by a scanner. The participants were aware of this, and they were asked about the rights of the people not able to or not willing to use new security technologies. The participants are reluctant to accept that people who are not able to or not willing to use new security technologies are discriminated when using public services. Slightly less than half of the participants will not accept *any* consequences for these two groups.

If this demand should be met, security technologies would have to be optional. This, however, presents a dilemma – when some people can legally avoid the technologies, the effectiveness of the technologies may be reduced drastically, but compulsory exposure to security technologies will be at odds with the democratic opinion.

The Spanish participants were very aware of this problem in their discussion. Around 80 percent of the Norwegians were in favour of forcing the objectors to accept new security technologies, whilst fewer than 40 percent the Austrians and Hungarians were willing to do this.

Chapter 6   Conclusion

This concluding chapter consists of three parts. The first part briefly summarises a number of important issues that divide the participants across the six countries. The second part consists of attitudes and opinions that are supported by the *vast majority* of the participants. A *vast majority* entails that 80 percent or more of the participants in the six countries have backed these conclusions in the relevant questions in the questionnaire. What is considered relevant is also based on what the participants have emphasised in the group discussions. Finally, this chapter lists a number of democratic demands that the participants have emphasised.

6.1   Important issues which differentiate he participants

Overall, the participants are highly nuanced in their perception of and attitude towards privacy and security. They are split when it comes to whether the security of the society is dependent on security technologies or not and whether the technology should be used, if it is available.

Another issue that differentiate the participants is trust in governmental institutions. On the one hand, Norwegian and Danish participants show great trust in the state and the official institutions. On the other hand, Spanish and particularly Hungarian participants have little trust in their official institutions and the public servants. This is important, because these are the institutions and persons that manage the security technologies.

6.2   Emphasised as important by the vast majority

Even though the six interview meetings have been conducted in six different countries with different backgrounds and different basic understandings of security and privacy it is possible to draw some conclusion that are common for the vast majority of the participants across the six countries.

The participants find it uncomfortable to be under surveillance. They also demand that privacy in principle should not be violated, and most participants cannot accept consequences – in the name of security – for fellow citizens who are unwilling or unable to use security technologies. However, there are a number of exceptions that make security technologies and privacy infringements acceptable.

It is possible to draw some conclusions on what privacy infringing use of security technologies the participants do not want to trade for security. It is also possible to draw conclusions on a number of exceptions that make the use of security technologies acceptable.

6.2.1   Basic limits of acceptability

The threat of terror as such does not justify privacy infringements
In general, the participants do not consider the threat of terror to be reason enough for implementation of security technologies or other privacy infringing measures. To a certain degree, this is surprising and indeed noteworthy in the light of anti terror legislation that has been implemented in many countries since September 11th 2001.

Another interesting point is that prevention of serious crime seems to be more important to the participants than prevention of terrorist attacks. The participants simply do not consider the threat of terror to justify the use of a number of privacy infringing security technologies.

Physically intimate technologies are unacceptable

Technologies that target the body make the participants feel uncomfortable. Cameras in dressing rooms and the naked machine are two examples of this unacceptable intrusion into the most private sphere.

Misuse of technology must be prevented

It is not surprising that misuse of technology is considered unacceptable. What is more interesting is that the citizens are convinced that security technologies *will* be misused. Definitely by criminals and commercial interests and, according to a majority of the participants in some of the six countries, by the state as well.

Function creep is not acceptable

It is not acceptable to use security technology or collected data for other things than the original purpose – known as function creep. If a technology is implemented with a specific target or function, it is not acceptable that the technology over time is used for other privacy infringing security purposes. This is valid for prevention or investigation of crime and terror as well.

6.2.2   What makes security technologies more acceptable?

Proportionality between security gain and privacy loss

The question of proportionality can be briefly summarised to two points: whether the security technology in question is effective, and whether the privacy infringement caused by the technology is justified by the threat.

Overall, effectiveness increases acceptability. The more effective the participants find the technology to be in relation to prevention and, to a certain degree, investigation; the easier it is for them to accept the privacy infringements caused by the technology.

In places or situations considered to be a 'danger spot' security technologies are much more accepted. Danger spots are places with high crime rates, e.g. dark alleys, and places considered to be vulnerable to terror, e.g. airports.

Court order

A court order renders the use of highly privacy infringing technologies like eavesdropping and location technologies acceptable. These measures are considered to be effective tools for police work but without a court order they are unacceptable.

It should be noted that some security technologies are considered to be so privacy infringing that not even court orders justify the use of them.

Strict control

Strict control of the individuals handling personal data collected via security technologies is essential for the participants. There must be very strict control to prevent misuse by the people with access to this data.

Privacy infringing security technologies must be the last option

Privacy infringing security technologies should only be implemented, if alternative solutions have been considered. Non-technological alternatives must be measured and found less effective prior to implementing privacy infringing technologies.

6.2.3   Democratic demands

Public debate

Decisions on implementing new security technologies or measures must always be based on a transparent decisions-making process. More important – before these kinds of decisions are taken, there must always be an informative and involving debate.

Broad involvement

All relevant parties, including experts and human rights organisations, must be heard prior to important decisions on security and privacy.

Always analyse privacy impact

Before implementing new security technologies the privacy impact of the technologies must be analysed thoroughly. Funding of research projects on new security technology should also be dependent on an analysis of the possible privacy impact.

Overview of Annexes

Additional information and data are provided in a separate document containing the following annexes:

- Annex 1 – Method handbook

- Annex 2 – Composition of participants

- Annex 3 – Scenarios

- Annex 4 – Questionnaire and interview guide

- Annex 5 – Frequency tables