



Security Research

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 5.3 Danish Report - Interview Meeting About Security Technologies and Privacy

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

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



TEKNOLOGI-RÅDET



Legal notice:

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

Table of Contents	page
Preface	4
Executive Summary	5
1.1 <i>Boundaries of privacy</i>	5
1.2 <i>Recommendations</i>	5
Chapter 2 General Attitudes	6
2.1 <i>The participants' general attitude</i>	6
2.2 <i>Conclusion</i>	8
Chapter 3 Security Technologies	9
3.1 <i>Biometrics</i>	9
3.2 <i>Camera Surveillance</i>	9
3.3 <i>Scanning</i>	10
3.4 <i>Localization technologies</i>	11
3.5 <i>Data retention</i>	11
3.6 <i>Eavesdropping</i>	12
3.7 <i>Privacy enhancing technologies</i>	12
3.8 <i>Conclusion</i>	13
Chapter 4 Dilemmas of security and privacy	14
4.1 <i>Convenience when traveling</i>	14
4.2 <i>Prevention of terror</i>	14
4.3 <i>Locating of cars and movements</i>	15
4.4 <i>Privacy enhancing for all</i>	15
4.5 <i>Consequences for other</i>	16
4.6 <i>Conclusion</i>	16
Chapter 5 Democratic Issues	17
5.1 <i>Democracy and participation</i>	17
5.2 <i>Proposals</i>	18
5.3 <i>Participants own proposals</i>	19
5.4 <i>Conclusion</i>	19
Chapter 6 Additional Issues	20
6.1 <i>Do not focus too narrowly on the technologies</i>	20
6.2 <i>Impact of the event on the participants' opinions</i>	20
6.3 <i>The Danish context</i>	20
Annexes overview	21

Preface

Wednesday the 30th of May, the Danish Board of Technology hosted a so-called *interview meeting* at the meeting facilities of Østerport Station, Copenhagen.

28 participants heard a presentation, filled out a questionnaire and debated issues of new security technologies and protection of privacy. Subsequently, similar meetings were held in Germany, Norway, Austria, Spain and Hungary.

Purpose of the report

Interview meetings are one of the central elements in the PRISE-project, financed by the European Commission. PRISE will provide guidelines and support for security solutions with a particular emphasis on human rights, human behaviour and perception of security and privacy.

This report sums up the attitudes and arguments presented at the Danish meeting.

Choosing participants for the meeting

The participants were recruited with the purpose of having a differentiated group of participants. They were selected on the background of sex, age and educational level. 2000 invitations were sent out to randomly selected people aged 18-75 in the greater Copenhagen area. Out of the positive responses, a group of 36 people were selected. Not everybody showed up at the meeting, so even though the final group had 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 – for more details on the selection process, please refer to Annex 1.

Nevertheless, among the participants, one could meet people with very different backgrounds, e.g. a former prison guard, a designer, a hospital porter, students and civil engineers.

Public attention before the meeting

In the weeks prior to the meeting, there had not been great media attention on security technology, but there had been some debate on a survey that suggested that Danes were especially positive towards camera surveillance (CCTV) (see *Ritzau*: "Danskerne er vilde med overvågning" 10.05-07). The survey was discussed in various newspapers, e.g. *Politiken* May 25th.

Also, a couple of dilemmas, not previously discussed, received some media attention – notably the issue of surveillance of privates by privates (including *Urban* May 16th & *Nyhedsavisen* May 30th) and the issue of raised public responsibility for the security of the citizens which ensues from new technological possibilities of surveillance (*Ritzau* 16.05).

However, since none of these were large public issues, media coverage seemed only to have marginal impact on the attitudes and arguments at the meeting.

Executive Summary

The concept of privacy is not solid, rather it transforms according to the situation. It is tightly connected to the feeling of trust in the use and effect of the security technologies.

The participants in the interview meeting were split in two groups: A small majority that feels uncomfortable about the security technologies and wants to protect privacy, and a minority that has a positive attitude towards new security technologies. At the same time, most of the participants recognize the need for development of new security technologies in general the utility of the presented technologies in prevention and investigation of crime and terrorism.

The critical majority of the group questioned the effect of implementing new security technologies – they expected criminals to be able to circumvent these technologies or misuse these technologies for their own gains. They also expected a lot of the technologies to simply push crime into other areas.

The question of effect is also a question about *trust* in the institutions, as part of the group expressed views to the effect that security technologies were primarily implemented in order to induce a feeling of comfort for political reasons, but with little real effect. Also a majority expected governmental institutions to misuse the technologies and expressed fear of privacy intrusion by the individuals controlling the technologies.

Interestingly, a vast majority were unwilling to accept any consequences for people not able or not willing to use certain security technologies. This could democratically impair the utility of certain technologies, e.g. data retention, location and scanning technologies.

1.1 Boundaries of privacy

The boundaries of privacy seem to be dependent on at least four factors: a) The naked body is a clear boundary of privacy. b) People do not feel comfortable with technologies that make their data too recognisable to the individuals using the technology. c) Certain areas or places seem to be less private and, in consequence, more suitable for implementing security technologies. d) The seriousness of the crime also has a privacy factor. Smaller crime is a private affair and should not be targeted by security technologies. For example, the participants were very sceptical towards automatic speed control.

1.2 Recommendations

There was almost consensus on the need for a thorough democratic evaluation of new security technologies before they are implemented – the democratic debate should include human rights organizations and to some extent the developers of the technology. The final decision should be political, though.

More effort should be put into researching the effectiveness of the technologies, the privacy impacts of technologies and low-technological alternatives. Regulation of both development and use of security technologies is necessary.

Chapter 2 General Attitudes

2.1 The participants' general attitude

“If you have nothing to hide, you don't have to worry about security technologies that infringe on your privacy”. That is one of the statements that the participants were confronted with in the questionnaire. The response towards this statement is very illustrative for the general attitudes among the participants. The group proved to be divided in their attitude towards the statement – with a small majority being worried about their privacy (of the 27 participants, 11 completely or partly agree, 2 neither agree nor disagree and 14 partly or completely disagree with the statement). Among the participants one could find a smaller technology optimistic group and a slightly larger privacy worried group. This was reflected in the group discussions that were characterized by disagreement and much debate.

The optimistic participants did not have any problems with surveillance and registration:

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.

The worried participants pointed out that even though you are a law-abiding citizen, increased surveillance and registration can have some long-term consequences that are difficult to foresee:

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 cannot imagine the situation where registration could become a problem even though it is not in connection with anything criminal.

The attitudes among the participants towards security technologies in general are somewhat contradictory. On the one hand the majority of the participants think that it is uncomfortable to be under surveillance and that privacy should not be violated without reasonable suspicion of criminal intent (approx. 70 percent partly or completely agree with these two statements). On the other hand, the majority of the participants believe that to a certain degree the security of society is dependent on the development of new security technology. We found that participants without children generally appear to be more critical towards the implementation of security technologies and more concerned about their privacy. The same goes for participants who do not have tertiary education – no one in this small subgroup felt comfortable under surveillance. Male participants proved to be more skeptical than women, especially concerning questions on discomfort as a result of privacy intrusion – less than a third of the men agreed or partly agreed to the statement “If you have nothing to hide, you don't have to worry about technologies that infringe on your privacy”, while more than half the women did.

There is a general skepticism towards the effectiveness of security technologies. The questionnaire shows that a majority of the participants believe that many security technologies do not really increase security and that they are only applied to show that something is being done to fight terror. This can be seen as a rather harsh critique of the efforts being done to fight terror and as mistrust towards the authorities. It is also an expression of some doubts about the effectiveness of security technologies in general. This is again very contradictory to the fact

that more than half of the participants think that the security of society is dependent on the development of new security technologies.

In the group discussions the participants expressed their doubts:

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...

Already now there is a lot of security control in the airports, but there are still people hijacking airplanes.

You have to consider whether it is worth it. (...) You can look at it the other way around, if you are a terrorist, well you have to secure everything. All supplies. You can just pour bacteria in the drinking water that would kill us all. Really, there are lots of possibilities, and terrorists are not stupid either. (...) You can go on forever.

The participants are also worried about abuse of security technologies. The questionnaire shows that slightly more than half the participants believe that security technologies will be abused by governmental agencies and almost 90 percent of the participants believe criminals will abuse them. In the group discussions the participants expressed that in the end criminals will always find a way to abuse the technology. They also emphasized 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 maybe not the way it was intended. One participant compares it to the a-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.

Another type of misuse the participants focus much on is misuse by the individuals behind the technologies. There is a widespread concern among the participants about who has access to information and data from security technologies, and what they can use it for.

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!

The participants also foresee commercial abuse of security technologies by private companies. Both in connection to advertising and analysis of personal consumer habits and connected to questions of insurance coverage.

Some participants feel offended by the possibility of private surveillance of children and the elderly. One refers to the scenario in which Carla is being watched over by her son.

The last part, where Carla is being watched over by her son without knowing it herself, that's what offended me the most (...) That's when I thought; I would really be offended by that.

2.2 Conclusion

A predominant part of the participants feel uncomfortable about the security technologies and want to protect privacy. Furthermore, there is certainly a majority that believe that criminals, commercial interests and the state alike will abuse the technologies and especially the people controlling the technologies are a cause of concern for the participants.

On the other hand there is a tendency towards wanting more and new technologies to enhance security. Developing and implementing new, effective security technologies that increase security without infringing upon privacy too much is part of the way to avoid conflicts. But the attitudes expressed at the meeting also stressed the importance of assuring trust in the institutions implementing and controlling new security technologies.

Chapter 3 Security Technologies

When we concentrate on specific security technologies, we find that the attitudes and opinions are more nuanced and differentiated. In the following we will go through the participants' attitudes towards these specific security technologies.

3.1 Biometrics

The use of biometrics for access control divided the participants into two groups. Approximately 40 percent of the participants will not feel comfortable, if any kind of biometrics is used, while the rest feels comfortable about the use of iris, fingerprint and, to a lesser extent, facial recognition.

When the technology is connected to specific situations and places it becomes more acceptable to the participants. The questionnaire reveals that a majority of the participants can accept the use of biometrics in airport and border control (approx. 60 percent of the participants). While a minority of approximately a quarter of the participants can accept biometrics in banks, bus and train stations, sports arenas and stores. As one of the participants who were positive towards biometrics expressed it:

I can clearly see the advantage of them (biometrics) when flying. Maybe it is a bit excessive to use it for bus transport. A little overkill (...) but it is security for all of us. So why not?

And when the participants compared the use of biometrics to some of today's security measures they found that:

It makes more sense than having toothpaste in a plastic bag.

Even though biometrics have a high degree of acceptance in airports and border control, the predominant part of the participants feel insecure using the biometric passport because of the risk of biometric data being stolen. This should also be seen in the light of the fact that the participants expressed some uncertainty as to what identity theft is, how big a risk using biometric passports poses and what the consequences of identity theft would be.

Another possibility with biometrics is registration of biometric data in a central database as a step to fight crime. The citizens are divided into to almost even groups of for and against such a register. The group discussions indicate that the thought of a DNA-register is quite unfamiliar to the participants, even though such a register is in existence today. In the group discussions the participants do not dwell very much upon this, but one participant says about a DNA-register:

As long as it is only used in connection with the investigation of crimes. It makes it very easy to exclude people (as suspects).

3.2 Camera Surveillance

Possibly as a result of its familiarity and iconic status, camera surveillance was the most discussed technology in the group discussions, and also the technology that most participants

have a positive attitude towards. The group discussions revealed that the participants find that camera surveillance has the potential to prevent crime as well as being a helpful tool in the investigation of specific crime or terrorist attacks that have occurred.

The questionnaire answers supported the high degree of acceptance of camera surveillance revealed in the discussions. More than four fifths of the participants think there is either an appropriate number of surveillance cameras in society in general or that there should be more cameras (11 participants think it appropriate and 11 wanting more). All the participants can accept the surveillance in airports, more than 90 percent can accept it in banks and at bus and train stations, Three quarters can accept in sports arenas and other crowded areas and two thirds of the participants can accept camera surveillance in stores.

As one participant argues:

TV surveillance in the public space – though not in restrooms and fitting rooms – but in other places I don't see anything wrong with that. It can help identify criminals, and anyway you normally wouldn't do anything in public that you wouldn't want others to see. So I can't see anything wrong with that.

There are limits though; only a minority of the participants can accept surveillance in all public places and in fitting rooms to prevent theft. The naked body seems to be too private – one participant formulates it very precise:

Not inside my intimate sphere!

At the same time, there seems to be some ambivalent feelings when it comes to whether camera surveillance makes one feel more secure. The group discussions dealt a lot with this and the main issue was whether surveillance provides more security or more mistrust. There were also participants who pointed out that there is no sure evidence of the effect of camera surveillance, especially not the preventive effect.

One decisive factor when it comes to the acceptance of camera surveillance is whether it is passive or active cameras. The group discussions showed that the main part of the participants could accept passive cameras where the recordings are only looked through in case of an incident. But there is some uncertainty as to whether you can trust that:

If you can always be sure that the information, the little peace of film and the little thing that is registered can never be abused and only be used to catch the bad guy (...) then it is okay. The problem is that you can never ever be sure of that.

Active cameras seem much more privacy infringing, probably because someone is in the other end actively watching you and evaluating your actions.

3.3 Scanning

The participants primarily find scanning acceptable in airports. They find that scanning is an acceptable tool for prevention of terror. A majority can accept scanning of luggage by x-ray, scanning for metal objects and body-scanning where images and hidden objectives are projected onto a mannequin. Only when it comes to the naked machine do almost all participants opt out. They obviously find that the naked machine goes beyond the bounds of propriety.

3.4 Localization technologies

Locating mobile phones and locating cars does not seem to be that controversial for the participants, as long as the location is either based on a court order, connected to an accident or with the purpose of locating a stolen car – all accepted by approximately three quarters of the participants. For these purposes many participants find that both eCall and the locating of mobile phones is a very positive way to use security technology.

Using eCall for speeding control and automatic speeding tickets is a controversial subject. On the one hand it is recognized that it can increase traffic safety, but on the other hand it is also seen as a major infringement of privacy. The questionnaire shows that it is accepted by a little more than a third of the participants (10 out of 27). But the predominant part of the participants thinks that installing eCall in new cars should either be optional or possible to deactivate. This is especially interesting; because it raises the question of public accept of misdemeanours, such as speeding. When implementing new security technologies, it might be important to define the crimes targeted very clearly to insure public acceptance.

The majority of the participants find the possibility of locating cars and mobile phones to be privacy infringing and at the same time a good tool for police investigation and prevention of crime and terror. The group discussions underlined that getting a court order is the decisive factor of acceptance when the police is using localization technologies.

3.5 Data retention

Data retention and scanning and combining of personal data from different databases can be used for both investigation and prevention of crime and terror. The questionnaire indicates that retention, scanning and combining of data is acceptable for the majority of the participants (more than three quarters of the participants) as long as the purpose is *investigation* of specific terrorist attacks or crimes that have occurred. When it comes to *prevention* only a quarter of the participants can accept the use of stored data.

At the same time the majority of the participants find data retention to be potentially privacy infringing. For example they state that traffic data from communication should not be stored for purposes beyond billing, which is the case at the moment. The opposition towards data retention can be rooted in the fear of data being used for something else than the original purpose, so-called function creep. In the questionnaire almost 80 percent of the participants indicate that function creep is a serious privacy problem. In the group discussions the participants expressed anxiety towards the possibility that someone can create a profile of them based on personal data from different databases. One participant uses the Danish central registration number to illustrate the point of function creep, because it is now being used for other things than when it was originally introduced. Another participant says:

You start from this little piece of information that when registered could be unimportant. But because you suddenly identify it as being important, you can go back and piece all other kinds of unimportant information together and connect it to a person.

In general it seems that data retention is difficult to comprehend. The part of the group who either uses e-mail or the Internet every day seems much less worried about registration. This indicates that regular interaction with a given technology makes people more comfortable, which can be taken in to account when implementing new technologies.

Even though they are worried, about half of the participants think that scanning and combining of personal data is a good tool that the police should use for the prevention of terror. Some of the skeptical participants emphasize that the amount of data can also get too enormous and therefore become useless.

It is worth notice that 4 out of the 27 participants state that data retention and scanning of databases with personal information is never acceptable. At the same time the majority of the participants find it unacceptable for governmental institutions to store all data they find necessary for security reasons. This suggests that the participants find that data retention involves some serious privacy problems.

This is also the impression one gets from the group discussions where many participants expressed their worries about the growth in data retention. Some participants point to the problem of who has access to this data.

The hardest dilemma is who should have access to all this data about me and the citizens...

However, other participants find this worry exaggerated. Instead they question the idea that anyone should have a private interest in looking at the data of ordinary people.

3.6 Eavesdropping

As is the case with localization technologies it is also the court order that is the decisive factor when it comes to eavesdropping. The questionnaire reveals that more than 80 percent of the participants can accept eavesdropping as a means of prevention and investigation of both crime and terror as long as there is a court order authorizing it, while only about a quarter can also accept it without 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.

As with other technologies a majority of the participants find eavesdropping to be a good tool for police investigation but also privacy infringing.

3.7 Privacy enhancing technologies

The majority of the participants feel that Privacy Enhancing Technologies (PET) are a necessity in today's society to preserve privacy (17 out of 27 participants agree to this in the questionnaire). When asked what technologies they thought should be accessible, more than a third of the participants did not know. This indicates a large degree of uncertainty about the PET that could be due to a lack of knowledge of these technologies or the way they work and the implications they can have. The most preferred PET is encryption programs (14 participants); while a minority of the participants thinks that anonymous calling cards and identity management should be legally accessible (respectively 6 and 8 out of 27).

3.8 Conclusion

The most discussed technology in the group discussions was camera surveillance, and there seems to be a very high degree of acceptance of cameras as long as they are passive and not active cameras.

Generally, surveillance and access control technologies are accepted in certain defined places, especially in airports. The same goes for scanning technologies. The places, in which the participants accepted these security technologies, are places where there is a perceived danger *and* it seems convenient. For example security checks at places that are not part of everyday life, such as airports and border crossings, do not appear to cause as much hassle as a security check on the daily bus route. Finally the body marks a clear line of privacy for most of the participants that should not be crossed by security technology.

For many of the technologies (localization technologies, data retention, eavesdropping) there are some ambivalent feelings among the participants. On the one hand they find the technologies to be good tools for prevention and investigation of crime and terror, but on the other hand they think that the technologies are privacy infringing, and most participants do not like that. This is an obvious dilemma for the participants that, in some situations, they can handle by leaning towards the demand for a court order to authorize the use of these measures. This central dilemma stresses the importance of securing trust in the institutions handling the security technology.

Another not so surprising observation is that the more familiar people are with the technologies, the easier it is for the participants to accept them. Furthermore, when the use of different security technologies are connected to places where there already is a high degree of control, the participants also find the use of the technologies easier to accept. This could indicate that acceptance of different security technologies is very much a matter of getting familiar with and accustomed to them.

Chapter 4 Dilemmas of security and privacy

In the questionnaire the participants were confronted with a series of dilemmas. Some of these dilemmas were also debated in the group discussions.

4.1 Convenience when traveling

First the participants were confronted with the dilemma of convenience when traveling versus protection of privacy. In relation to traveling with the underground a majority of the participants are not willing to give up any privacy for the convenience of easy payment. Some participants can accept for example to use fingerprints for registration and easy payment, but at the same time it must be optional and not the only form of payment. Convenience when traveling in public transport does not seem to be more important than privacy to the majority of the participants.

When it comes to traveling by plane the participants are far more willing to accept loss of privacy for convenience. Only about a third of the participants cannot accept any loss of privacy in exchange for fast and convenient check-in in the airport. The rest accepts different forms of convenient, but privacy infringing security technologies: The technologies and means that are accepted are thorough pre-registration and use of biometrics, going through the naked machine and being scanned for sweat, body heat and heart rate – each technology accepted by a third of the participants. We find that frequent flyers are more willing to use new security technology – once more this indicates that familiarity with the situations and technologies is an important factor of acceptance.

The reason for the larger approval of security technology in airports is probably the fact that the participants are more used to privacy losses when traveling and that airport security checks takes longer time. There is less privacy to give up and more convenience to gain at the airport compared to ordinary public transportation.

4.2 Prevention of terror

The dilemma of prevention of terror versus loss of privacy is complex. Active surveillance cameras and automatic face recognition (AFR) in airports and train stations may be able to prevent terrorist attacks, but they could also cause innocent people to be mistaken for terrorists and taken aside for questioning. The participants are divided in their attitude towards this dilemma. Around 25 percent of the participants do not feel that active cameras and AFR should be used at all, around 40 percent of the participants think that the technologies should only be put to use if no one is mistaken for a terrorist and around 30 percent can only accept a low rate of people mistaken for terrorists. In addition, the majority of the people who can accept this kind of surveillance state that it should be used in places that are very vulnerable to terrorism or where many crimes have occurred.

Some participants focus on the consequences, if all travelers going to work and changing at the central station would have to go through a security check.

It would have enormous consequences if you were to security check all passengers going to work and changing trains at the main station.

Another technology that can be used in the prevention of terror is the scanning and combining of data from different databases with personal information in order to detect suspicious patterns. When it comes to the police searching databases with personal information, the participants are clearer in their attitude towards the dilemma. 19 percent or 5 out of 27 can accept police searching databases, 5 can never accept it and the remaining 17 can only accept the use of the technologies, if the data is made anonymous and only a court order can have the identity revealed. If the data is not made anonymous, most participants find the possibilities frightening. As one participant says:

It can be out together in some database and then some total profile of me is stored. I find that very frightening, and it makes me feel more insecure than some terrorist with a bomb.

Data retention and combining of data from different databases is something that most participants find very privacy infringing. They strongly suggest that there should be strict regulation on the possibilities of searching and combining personal data from different databases.

4.3 Locating of cars and movements

The eCall technology can register the movement of cars. This registration can be used for different purposes and with different degrees of privacy infringement. The participants find the original purpose, which is registration and reporting of the cars' positions in the case of accidents, to be a very positive thing.

Police can also use the eCall system for two other purposes. One is the possibility of activating the eCall system and locating a car to prevent crime or terror – the other is automatic giving of speeding tickets. Even though traffic, and especially speeding, causes more deaths than terrorism, the participants are far more willing to let the police trace vehicles to prevent terrorist attacks than using it for giving speeding tickets. There seems to be something sacred about the right to speed, and the participants find it very privacy infringing not to be able to speed without getting a ticket. This stresses the importance of guaranteeing that security technologies are not used to target smaller crime.

4.4 Privacy enhancing for all

Privacy enhancing technologies can be used by ordinary people to protect their privacy, e.g. when communicating by phone or using the Internet. But these technologies can also be used by criminals and terrorists and might make police investigation and prevention of terror and crime more difficult. The predominant part of the participants are willing to accept legal use of encryption even though it might make police investigation and prevention of terror and crime more difficult. When it comes to anonymous calling cards and anonymity when using the Internet, it becomes more difficult. Less than half the participants can accept that these technologies are legal, if they make police investigation and prevention of terror and crime more difficult. When it becomes case specific, it is even less acceptable to the participants. If the consequence is that persons searching for bomb instructions cannot be traced by police only a third of the participants can accept Internet anonymity, that number is reduced to less than a fifth of the participants when the consequence is that persons searching for child pornography cannot be traced by the police.

Privacy enhancing is important to the majority of the participants. The participants are willing to accept that police investigation of crime and terror becomes more difficult, but some consequences are more difficult to accept than others (e.g. child pornography which is a very sensitive subject). Internet anonymity does not seem to be as important as anonymity when communicating by phone. This could indicate that the participants consider using the Internet less private.

4.5 Consequences for other

The last dilemma the participants were confronted with was what consequences they would accept for other people, if a security technology could provide greater security. The possible consequences were exclusion from public services or trouble using public transport and the participants were asked to distinguish between people who were *unable* to use the technology and people who were *unwilling* to use the technology.

The predominant part of the participants are not willing to accept any consequences neither for people who are not able to nor for people who do not want to use the technology. The minority that could accept some consequences would mostly accept consequences for people unwilling to use the technology, while only slightly above 10 percent could accept consequences for people unable to use technology. This indicates a feeling of solidarity for both unable and unwilling persons, and that this solidarity is more important than security. Probably the participants find it easier to imagine being excluded from societal goods than the consequences of a terrorist attack. This complicates implementation of new security technology in some areas. For example, we have located a distinct group of people who will not allow data retention or scanning of databases. If these people are excluded from some services, it will conflict with the opinion of the majority, but if it is legal to circumvent the technology, the effect of data retention and scanning appears insignificant.

4.6 Conclusion

The dilemmas of how to use security technologies are complex. One thing is looking at the technological possibilities; another is looking at the concrete use of the same technologies and the possible consequences.

Convenience when traveling at the expense of privacy can only be accepted by the majority when traveling by airplane, not in other public transportation. In relation to prevention of terror, the participants can accept some use of security technologies, but if it becomes privacy intruding, they want it to be authorized by a court order. In general, privacy enhancing technologies are not considered very valuable, if they make police investigation of crime and terror more difficult. The most accepted PET is encryption. And finally the majority of participants are not willing to accept any consequences and inconveniences for people who are unable to use the security technologies nor for people who refuse to use them.

Chapter 5 Democratic Issues

5.1 Democracy and participation

Decisions about development and implementation of new security technologies can potentially have significant influence on everyday life of citizens. Therefore decisions about security technologies should be made on a democratic background. The question is to what extent: Who should be involved in the considerations, in what decisions and in what way. The participants were confronted with this issue.

The participants show a high degree of trust in the representative democracy. They believe that the politicians they have elected should make this kind of decisions, but they also think that public debate and public hearings must be part of the decision process when taking decisions about new security technologies. Only a few participants partly agree that questions about security and privacy are too complicated to involve the general public. The general attitude is illustrated by this quote from the group discussions:

After a broad public debate it would be reasonable if the politicians made the decisions. That is our democracy.

Some participants wish for more influence on the decisions and suggest some form of public voting (referendum) on important security/privacy issues. All participants agree that involving the citizens is very important, but after some debate most participants agree that it will be better to focus on public debate and the politicians getting some indication of the public attitude before taking decisions.

You could have the citizens give an indication of what direction we should take, but then I think you should say: "That was it". Then a team of experts or a committee must fine-tune it. You cannot put it out to the public.

Another thing that most participants find important is that people with expert knowledge of the technologies and their possible consequences advise politicians.

Because politicians only act on basis of a political perspective.

When it comes to involving other parties in important decisions about security and privacy, almost all the participants (more than 90 percent) agree that human rights organizations must be involved. The debates in the group discussions indicate that the participants see the human rights organizations as spokesmen for the individual privacy.

Even though the participants are more divided about involving developers of security technologies the majority (15 out of 27) believe they should be involved. The reason for this is the expert knowledge of the technologies that these developers have.

It is essential to note that almost all the participants find it very important that alternative solutions are included in the debate.

5.2 Proposals

At the end for the questionnaire the participants were asked to evaluate the importance of four proposals for privacy enhancing use of security technologies. 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 unsuspecting individuals must be anonymous until identification is authorized by court order	20	3	2	0	2
Only authorized personnel shall have access to collected personal data	25	2	0	0	0
Prior to implementing, new security technologies must be checked for privacy impact	19	7	1	0	0
Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts	12	6	5	2	2

The two first proposals aim at regulating the use of security technologies. Earlier in this report we have seen that the participants find access to personal data collected by security technologies to be very sensitive. The proposal that only authorized personnel should have access to this data is the one that most participants find to be of high importance. Also the proposal about anonymity until a court order is given is evaluated as important by the citizens.

The two other proposals are aiming at the steps prior to implementing new security technology. The proposal about a privacy impact check prior to the implementing of new technology is evaluated as having some importance. The proposal on funding of research projects depending on analysis of privacy impacts does not seem to be as important to the participants as the other three proposals. This could be because the participants do not think it is possible to control the development of new security technologies anyway. This opinion was aired in the group discussions:

If someone wants to buy, then someone wants to produce it. That's the way the market works

Others, however, disagree with this opinion and find regulation of development to be both important and possible.

5.3 Participants own proposals

The participants also made their own proposals as to how to enhance privacy in the development and use of security technologies.

Regulation of development:

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.

Limited power to individuals behind the technologies:

Then as far as possible you have to guard against misuse. Individuals should have as little power in the systems as possible.

Legislation that limit the use of security technologies:

You must have some rules on where you can use this technology.

5.4 Conclusion

The participants trust the representative democracy and think that in the end politicians must make the decisions on what and how to implement new security technologies. However they find it important that the citizens are involved in a public debate about these issues. They also want both human rights organizations and to a lesser extent the developers of the technology to be heard before the politicians make their decisions.

One other important conclusion is that the participants find it important that alternative solutions are included in the debate.

The participants found the proposals they were confronted with in the questionnaire to be of high importance, and they also contributed their own proposals during the group discussions: proposals on how to regulate development and use of security technologies.

Chapter 6 Additional Issues

6.1 Do not focus too narrowly on the technologies

The subject of the interview meeting was the possibilities and privacy threats of new security technologies. But a couple of times during the group discussions participants touched upon the danger of focusing too narrowly at the technologies and considering them to be the only options in the fight against crime and terror. Some participants emphasized the need to look at non-technological solutions, e.g. improved street lighting or other alternatives instead of camera surveillance.

If you had two policemen patrolling, going around whistling, right. That would be ten times more effective than a video camera.

Others advocated focusing more on the possible downsides of the technologies and especially the possibilities of misuse before introducing these technologies.

It is not about how the technology can be used, it is about how it can be misused.

6.2 Impact of the event on the participants' opinions

At the end of the group discussions as well as the questionnaire, the participants were asked, if their opinion had changed as a result of their participation in the interview meeting. The questionnaire showed that the majority of the participants had not changed opinions, while 6 out of 27 participants had become more worried and 1 had become more positive towards security technologies. Some participants stated that they had come to give their opinion, not to change it.

On the other hand, many participants indicated that they had both learned a lot and gained interest in the subject by participating. They also expressed that it had been a positive experience to participate, and that there should be more sessions like this.

It has made me think more about the problematic of security.

It hasn't made me change my mind, but I can see that there has been developed something new that I wasn't aware of. There is definitely much more than I realized. There is also a lot that I would like get to know more about.

6.3 The Danish context

Some of the results in this report are likely to be a product of the Danish context. Denmark has been participating in the war in Iraq and is consequently a target of terror threats – some have been sentenced on the grounds of conspiring to commit terrorism. However, it is important to be aware that it is more than 15 years since there has been an actual terrorist attack in Denmark and that the country has never faced a major scale terrorist attack. It is possible that this makes Danes question the effect of the technologies more than other countries.

It is also worth noticing that Denmark has an old and sound democracy, and both politicians and especially public authorities enjoy a high degree of trust from the citizens. It is likely that the Danes show a greater trust in the control of new security technologies on this background.

Annexes overview

- Annex 1 – Participants' background
- Annex 2 - Program of the interview meeting
- Annex 3 - Material sent to the participants
- Annex 4 - Questionnaire and interview guide in national language
- Annex 5 - Transcript of group interviews in national language
- Annex 6 - Frequency tables
- Annex 7 - Comments from the questionnaire