PRISE
privacy • security

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 5.1 Questionnaire and Interview Guidelines

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

Author: Anders Jacobi,
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
LD10@datenschutzzentrum.de
www.datenschutzzentrum.de

Table of Contents   **page**

Preface

This deliverable is the English version of the questionnaire and the interview guidelines used for the participatory activities, the six national interview meetings. For each meeting the questionnaire and the interview guidelines have been translated into the national language. This English version has been the basis version that has been translated into Norwegian, German (for both Germany and Austria with slight adjustments to take into consideration language differences), Hungarian, Spanish and Danish. The six versions in national languages are made available as an annex to the reports from the national interview meetings.

First part of this deliverable is the questionnaire in chapter one, followed by the interview guidelines in chapter 2.

Chapter 1   Questionnaire on Security technology and privacy

Welcome to the PRISE project questionnaire survey on the attitudes towards security technology and privacy

In this questionnaire you will be presented with a series of questions. *Please circle the number next to the answer you want to give.* You must give only *one* answer to each question, except when it is specifically said that "you can circle more than one answer to this question". If you circle a wrong answer, just cross it out, and circle the correct one. You are more than welcome to ask questions along the way if you have any doubts about the meaning of questions.

Background Questions:

1. Sex

1. Male

2. Female

2. Age *(open)*

- Age: _____

3. Number of persons in your household, yourself included?

1. 1 person

2. 2 persons

3. 3 persons

4. 4 persons or more

4. Do you have children?

  1. Yes

  2. No

5. Are there any children living at home? *(you can circle more than one answer to this question)*

  1. No

  2. Yes, 14 years of age or younger

  3. Yes, more than 14 years old

6. What is your highest level of education?

  1. Elementary School - 7 years of schooling

  2. Intermediate School - 8 or 9 years of schooling

  3. Vocational training (skilled level/craftsman's training)

  4. Secondary school (high school graduation)

  5. Short-term higher education (less than 3 years of study)

  6. Medium length higher education (3 - 4 years of study)

  7. Advanced higher education (more than 4 years of study)

7. Please state your occupation (*open text box***)**

  - Occupation: _____

8. Do you live in a city or in the country?

1. Metropolitan area

2. Provincial town

3. Rural district

9. How often do you use a mobile phone?

1. At least once a day daily

2. At least once a week

3. At least once a month

4. Less than once a month

5. I never use mobile phone

10. How often do you write emails?

1. At least once a day daily

2. At least once a week

3. At least once a month

4. Less than once a month

5. I never write emails

11. How often do you use the Internet?

1. At least once a day daily

2. At least once a week

3. At least once a month

4. Less than once a month

5. I never use the Internet

12. How often do you travel by public transport?

1. At least once a day daily

2. At least once a week

3. At least once a month

4. Less than once a month

5. I never travel by public transport

13. How often do you travel by airplane (One return trip counts as one time)?

1. More than 5 times a year

2. 3-5 times a year

3. 1-2 times a year

4. Less than 1 time a year

5. Never

14. How often do you travel by car?

1. At least once a day daily

2. At least once a week

3. At least once a month

4. Less than once a month

5. I never travel by public transport

General Questions about security technology and privacy

Below you will find a number of the statements about security technology and privacy that appear in the public debate. To which degree do you agree with these statements?

For each statement please indicate to which degree you agree

- If you believe that the statement is completely right, circle 1 "Completely agree"

- If you believe that the statement is right, but have some reservations, circle 2 "Partly agree"

- If you find it impossible to assess whether the statement is right or wrong, circle 3 "Neither agree nor disagree"

- If you believe that the statement is wrong, but have some reservations, circle 4 "Partly disagree"

- If you believe that the statement is completely wrong, circle 5 "Completely disagree"

15. "The security of society is absolutely dependent on the development and use of new security technologies"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

16. "Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

17. "If you have nothing to hide you don't have to worry about security technologies that infringe your privacy"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

18. "When security technology is available, we might just as well make use of it"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

19. "Privacy should not be violated without reasonable suspicion of criminal intent"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

20. "It is uncomfortable to be under surveillance, even though you have no criminal intent"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

21. "New security technologies are likely to be abused by governmental agencies"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

22. "New security technologies are likely to be abused by criminals"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

Security technologies

In this section you will be asked about your attitude towards specific security technologies and their use. The grey text boxes give very short pieces of information about the technologies that are questioned subsequently. The boxes contain some of the same information about technologies as the boxes in the scenarios send out before hand. For further information about the technologies see the scenarios.

One part of these technology questions focuses on acceptable use of the technologies and to these questions it will mostly be possible to give more than one answer.

The other part of the technology questions is specific statements. For each statement please indicate to which degree you agree.

Biometrics

Biometric technology identifies individuals automatically by using their biological or behavioural characteristics. Biometrics can be used to control access to physical locations or to information (computers, documents). The most commonly used biometrics are fingerprints and facial characteristics.

Biometric image can be stored as the original image or in the form of a *template*, which is a digital representation of the biometric. For privacy reasons, it is recommended to only store the template, and discard the original image. However, in law-enforcement systems, like biometric passports, and facial recognition systems, the original image is often retained.

One of the major advantages with biometrics is that they are so strongly linked to a person. Biometric authentication provides better access control, and identity theft becomes a lot more challenging when personal data are linked exclusively to the right person. But this is also the greatest liability of biometric systems. Once a set of biometric data has been compromised, it is compromised forever.

Biometric passport

A biometric passport consists of the actual document with an embedded chip containing biometric data. The chip can be read by a reader at a distance.

Biometric passports have caused debate, because it is feared that the biometric information on the chip can be stolen by skimming (reading the information at a distance without the owner's knowledge) or by eavesdropping.

One challenge with biometric systems is finding the right balance between the False Acceptance Rate (FAR) and False Rejection Rate (FRR). *False acceptance* (or *false positive*) is when a system identifies an individual incorrectly. If the system fails to identify an individual that is registered, it is referred to as *false rejection* (or *false negative*).

23. What biometrics would you be comfortable using for access control? *(you can circle more than one answer to this question)*

1. Facial characteristics

2. Fingerprints

3. Iris recognition

4. I will not be comfortable using any biometrics for access control

5. Don't know

24. Where is using biometrics for access control acceptable? *(you can circle more than one answer to this question)*

1. Acceptable for security control in banks

2. Acceptable for airport security

3. Acceptable for security control in stores

4. Acceptable for border control

5. Acceptable for security control in central bus and train stations

6. Acceptable for security control in sport-stadium and other crowded places/events

7. Acceptable for security control in other private services not mentioned

8. It is never acceptable

9. Don't know

Specific statements about biometrics

25. "Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

26. "The use of the biometric passport makes me feel insecure because of the risk of my biometric data being stolen"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

Closed Circuit Television (CCTV)

CCTV surveillance with *active cameras* is when an operator watches the monitor and can control the camera (turn, zoom) to follow an individual or a situation that develops. Active cameras can be used with automated visual surveillance programs that use algorithms to detect suspicious motion or identify people by comparing their image to a reference in a database.

Passive cameras: These cameras record what happens in a specific spot (for instance in a kiosk) on a tape. The tape is viewed only if there is an incident, like a robbery, fight etc.

Automatic face recognition

Automatic face recognition systems are systems where a person's image is captured automatically and compared to a database for identification or authentication. Such systems are normally used to verify that a person is not on a list of for instance known criminals or terrorists.

Automatic Number Plate Recognition (ANPR)

ANPR systems read number plates picked up by CCTV and match them against a database. Systems for number plate recognition are in use in several countries. They are mostly related to toll booth passing or speed cameras, but they are also used to identify stolen vehicles.

Passenger scanning (*Naked machines*)

Technologies such as *backscatter X-rays or Terahertz radiation* have better penetration in materials than optics. This means that it can be used for detection and imaging of items concealed by clothing.

A "naked machine" utilises this type of technology to reveal if a person has weapons or explosives hidden on their body. There are different systems in use. Some reveal everything under the clothes – not just guns and explosives – hence the name. This type of airport security has been tested at Heathrow (Terminal 4) since 2004. Other applications take the images of concealed objects and project them onto a sexless mannequin.

27. Where can you accept CCTV surveillance? *(you can circle more than one answer to this question)*

1. In stores

2. In dressing rooms to prevent shoplifting

3. In central bus and train stations

4. In banks

5. In airports

6. In sport-stadium and other crowded places/events

7. In all public spaces

8. It is never acceptable

9. Don't know

28. How do you feel about the number of CCTV cameras in public spaces in general?

1. There should be more CCTV cameras in public spaces

2. The number of CCTV cameras in public spaces is appropriate

3. There should be less CCTV cameras in public spaces

4. There should be no CCTV cameras in public spaces at all

5. Don't know

29. Where is scanning of persons for detection of hidden items necessary for security reasons? *(you can circle more than one answer to this question)*

1. I schools

2. In central bus and train stations

3. In airports

4. In shopping malls

5. In public buildings (e.g. court)

6. It is never necessary

7. Don't know

30. What type of scanning would you find acceptable? *(you can circle more than one answer to this question)*

1. Scanning that reveal everything under the clothes

2. Scanning where images and hidden objectives are projected onto a mannequin

3. Scanning of body heat, sweat and heart rate

4. Scanning for metal objectives

5. Scanning luggage by x-ray

6. Scanning is not acceptable

7. Don't know

Specific statements about CCTV and passenger scanning

31. "CCTV surveillance makes me feel more secure"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

32. "CCTV surveillance infringes my privacy"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

33. "Scanning of persons for detection of hidden items is an acceptable tool for preventing terror"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

Locating technology

It is possible to calculate the approximate position of the user's mobile equipment by using known coordinates of for instance GSM base stations.

For more accurate positioning, satellite based systems are used:

GPS is short for *Global Positioning System*, which is the existing system. *Galileo* is planned to be fully operational in 2010. It will be more accurate than the GPS system, and it will have greater penetration.

eCall

The eCall device contains sensors that are activated after an accident. It calls the emergency number and communicates information about the accident, including the time, precise location, direction and identification of the car.

The device will not be permanently connected to a mobile communications network, it will only connect after it has been triggered. There is, however, concern that this could change, about the transmitting of additional data (for instance for insurance companies), and about possible unauthorised access to databases where eCall data is stored. From September 2009, all new cars in the participating countries will be equipped with eCall.

34. For what purpose is locating of mobile phones acceptable? *(you can circle more than one answer to this question)*

1. Police locating mobile phones of suspected terrorists and criminals based on a court order

2. Police locating any mobile phone without a court order

3. In case of emergency, e.g. an accident, lost child or disoriented person

4. It is never acceptable

5. Don't know

35. For what purpose is locating of cars acceptable? *(you can circle more than one answer to this question)*

1. Police locating cars of suspected terrorists and criminals based on a court order

2. Police locating any cars without a court order

3. Police locating stolen vehicles

4. Speeding control and giving speeding tickets

5. Automatic locating and calling of the emergency number in case of a car accident

6. It is never acceptable

7. Don't know

36. Should eCall automatically be installed in all new cars?

1. Yes

2. Yes, but it should be possible to deactivate eCall

3. No, it should be optional

4. No, it should never be installed

5. Don't know

Specific statements about locating technologies

37. "The possibility of locating all mobile phones is privacy infringing"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

38. "The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

39. "The possibility of locating all cars is privacy infringing"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

40. "The possibility of locating all cars is a good tool for the police in investigating and preventing terror and crime"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

Data retention

A database is defined as an organised collection of data. It is widely recognised that when different pieces of data about a person can be put together, it reveals more about that person than the information items viewed separately. An important privacy principle related to databases containing information about persons is therefore that only the data necessary to fulfil the purpose of the system should be collected, and that it should be deleted when it is no longer needed.

Lately, we have seen a trend where governments have wanted to store more data and connect database systems for purposes that are different from the original purpose, like security. The types of data most commonly referred to when data retention is discussed, is data related to ICT, such as communication data from phone, mobile phone and Internet traffic.

Total Information Awareness (TIA)

Total Information Awareness (TIA) was a program with the US Defence Advanced Research Projects Agency (DARPA). The TIA program contained three categories of tools - language translation, data search and pattern recognition, and advanced collaborative and decision support tools.

The goal of TIA was to predict terrorist attacks before they happen. The system was intended to scan private and public databases, as well as the Internet, for transactions that might be associated with a terrorist attack. The US Congress stopped the funding of TIA in September 2003, but many of the programs within the system live on under different names.

Function creep

Database systems are vulnerable to so called function creep, that is the use of the data for something other that the original intention. An example of such function creep was seen when the Norwegian data

base of asylum seekers – which also contains biometric information like fingerprints – was opened to the police in criminal investigations. The original intention of the data base was to help establish the identity of asylum-seekers.

41. For which of the following purposes do you find data retention of communication traffic data acceptable? *(you can circle more than one answer to this question)*

1. For prevention of terrorist attacks in general

2. For investigation of specific terrorist attacks that have occurred

3. For prevention of crime in general

4. For investigation of specific crimes that have occurred

5. For commercial purposes

6. It is never acceptable

7. Don't know

42. For which of the following purposes do you find scanning and combining personal data from different databases acceptable? *(you can circle more than one answer to this question)*

1. For prevention of terrorist attacks in general

2. For investigation of specific terrorist attacks that have occurred

3. For prevention of crime in general

4. For investigation of specific crimes that have occurred

5. For commercial purposes

6. It is never acceptable

7. Don't know

Specific statements about data retention

43. "Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

44. "Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

45. "Scanning of and combining data from different databases containing personal information is privacy infringing"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

46. "Scanning of and combining data from different databases is a good tool for police to prevent terror"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

47. "Databases being used for something else than the original purpose is a serious privacy problem"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

Eavesdropping

Different applications can be used for monitoring citizens and interaction between citizens, either over the internet, telephone network or in defined areas. One form of eavesdropping is often referred to as *wiretapping.* This is essentially to install a listening device in the path between two phones that are part of a conversation. Wiretapping can be set up on the suspect's telephone or on the telephones of persons he or she is expected to contact.

An extended version of wiretapping is to more indiscriminately tap all communication lines (phone, mobile, Internet) in search of conversations that may be of interest.

48. For which of the following purposes is eavesdropping acceptable? *(you can circle more than one answer to this question)*

1. For prevention and investigation of terrorist attacks *with* a court order

2. For prevention and investigation of terrorist attacks *without* a court order

3. For prevention and investigation of crime *with* a court order

4. For prevention and investigation of crime *without* a court order

5. For commercial purposes

6. It is never acceptable

7. Don't know

49. What methods of eavesdropping is acceptable?

1. Police eavesdropping all communication lines in search of conversation that may be of interest

2. Police eavesdropping lines of persons that suspect's is expected to contact

3. Police eavesdropping lines of suspects

4. Eavesdropping is totally unacceptable

5. Don't know

Specific statements about eavesdropping

50. "Eavesdropping is a good tool for police investigation"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

51. "Eavesdropping is a serious violation of privacy"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

Privacy enhancing technologies

Technologies that contribute directly to preserving privacy are known as Privacy enhancing technologies (PETs).

Anonymisation is one such PET. There are services that can enable anonymous electronic communication for regular users. Such technology hides the connection between the user and the traces he or she leaves behind, and can therefore prevent unwanted identification

Identity management is also a form of PET: In some cases you don't want to identify yourself, but use a pseudonym (for instance in forums on the internet). In order to make it more difficult to match data, it can be a good idea to have different user names (which do not reveal your identity) and passwords for different purposes. Identity management systems assist people in keeping track of their different user names

Encryption is about distorting content to make it illegible to others. Because all electronic communication is vulnerable to eavesdropping or manipulation, it is in many cases crucial that the communication is taking place on encrypted lines, or that the content being transmitted is encrypted.

52. What kinds of privacy enhancing technologies should be legally available for all citizens? *(you can circle more than one answer to this question)*

1. Anonymous calling cards

2. Encryption programmes

3. Identity management

4. No privacy enhancing technologies should be legal and available

5. Don't know

Specific statements about privacy enhancing technologies

53. "Privacy enhancing technologies are a necessity in today's society to preserve privacy"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

54. "Privacy enhancing technologies should not be legal if they make police investigation and prevention of terror and crime more difficult"

1. Completely agree

2. Partly agree

3. Neither agree nor disagree

4. Partly disagree

5. Completely disagree

Dilemmas in the use of security technology

We will now present you with a number of specific dilemmas in the use of security technology in proportion to the privacy consequences. For each dilemma we would like you to think about advantages as well as disadvantages and then answer the question. *You can give more than one answer to all of the questions in this section.*

55. Using your fingerprints in the underground to register when and where you are travelling could make it possible to automatically deduct the payment from your account. This would make payment a lot easier, but includes registration of your travelling and using your fingerprint for authentication. How would you feel about that? *(you can circle more than one answer to this question)*

1. I can accept registration of my travelling and using my fingerprints in the underground because it makes payment easier

2. I can only accept it if my fingerprints are stored only as a template and cannot be reconstructed

3. I can only accept it if the registration of my travelling is deleted after payment

4. Using fingerprints should be a possibility, but not the only form of payment

5. I would never use my fingerprints as identification in the underground

6. Don't know

56. Thorough registration in an airport database and acceptance of certain security technologies that can be regarded as privacy infringing, can make fast check-in at the airport possible. What security technologies and privacy infringements would you accept for faster check-in at the airport? *(you can circle more than one answer to this question)*

1. I would accept being thoroughly checked and registered in a permanent airport security database and then using biometrics for authentication on all further occasions

2. I would accept going through the "naked machine"

3. I would accept being scanned for sweat, body heat and heart rate

4. I would not give up privacy for fast and convenient check in at the airport

5. Don't know

57. Active CCTV surveillance cameras and automatic face recognition where faces of people are checked against a database of known terrorist are security technologies that can be used to prevent terror attacks, e.g. in airports or train stations. These security technologies could possibly prevent a terror attack, but the effect is not proven. They could also lead to innocent persons being mistaken for terrorists and taken aside for questioning. At what cost should these technologies be put to use? *(you can circle more than one answer to this question)*

1. Active cameras and automatic face recognition should be used no matter how many innocent persons are mistaken for terrorists

2. Active cameras and automatic face recognition should be used but only with a low rate of people mistaken for terrorists

3. Active cameras and automatic face recognition should only be put to use if no one is mistaken for terrorist

4. Active cameras and automatic face recognition should only be used in places where many crimes have occurred or that are very vulnerable to terror

5. Active cameras and automatic face recognition should not be used anywhere

6. Don't know

58. New technology makes it possible to scan and combine data from different databases containing personal information with the purpose of detecting suspicious patterns in personal communication and Internet use. The purpose is to foresee and prevent terror attacks, but it means scanning personal data from innocent persons. What police access to search and combine different databases do you find acceptable? *(you can circle more than one answer to this question)*

1. Police should have access to search and combine all databases for suspicious patters that can identify possible terrorists

2. Police should only have access to search and combine databases if the data is anonymous and only a court order can have the identity revealed

3. Police should never be allowed to search and combine databases for suspicious patterns

4. Don't know

59. The technology eCall could be installed in all new cars in order to call an emergency number in case of an accident. The eCall technology could also be used to locate cars for other purposes, e.g. if they are stolen or if they are used for crime or terror, but this requires that the movement of cars with eCall is registered at all times. What use of eCall do you find acceptable? *(you can circle more than one answer to this question)*

1. I find it acceptable that eCall can be activated by the police to locate a car if necessary to prevent crime or terror

2. I find it acceptable that eCall is active at all times and can be used to give speeding tickets

3. I find it acceptable that the movements of my car is registered at all times

4. eCall should not be used for any other purposes than reporting accidents

5. Installing of eCall in cars should be voluntary

6. Don't know

60. Privacy enhancing technologies (PETs) can contribute directly to preserving privacy when communicating by phone or mail and when using the Internet. But PETs can also be used for criminal activities and by terrorists. If the purpose is to preserve ordinary peoples privacy, what risks are you willing to accept for legal access to use of PETs? *(you can circle more than one answer to this question)*

1. I can accept legal anonymous calling cards, even though it might make police investigation and prevention of terror and crime more difficult

2. I can accept legal use of encryption, even though it might make police investigation and prevention of terror and crime more difficult

3. I can accept Internet anonymity, even if it means that persons searching for bomb instructions can not be traced by police

4. I can accept that Internet anonymity means that persons searching for child pornography can not be traced by the police

5. I can not accept any PETs that might make police investigation and prevention of terror and crime more difficult

6. Don't know

61. If a security technology provides high security, what consequences can you accept for people who are not able to use the technology and for people who refuse to use the technology for privacy reasons? *(you can circle more than one answer to this question)*

1. I can accept that people who refuse to use the technology for privacy reasons are excluded from using some public services

2. I can accept that people who are unable to use the technology are excluded from using some public services

3. I can accept that people who refuse to use the technology for privacy reasons are in some ways impeded when travelling by public transport

4. I can accept that people who are unable to use the technology are in some ways impeded when travelling by public transport

5. I can not accept any consequences for people who refuse to use the technology for privacy reasons

6. I can not accept any consequences for people who are unable to use the technology

7. Don't know

Democratic issues

In the following section you will be presented to some statements about democratic issues concerning new security technologies. Who should be allowed to exert an influence in the matter of security technology and privacy and how?

To which extent do you agree or disagree in the following views – please indicate your opinion of each point of view. Please give only one answer to each question.

62. "Politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies"

1. I completely agree

2. I partly agree

3. I neither agree or disagree

4. I partly disagree

5. I disagree

63. "The subject of security and privacy is so complicated that it makes no sense to include the general public in discussions of this issue"

1. I completely agree

2. I partly agree

3. I neither agree or disagree

4. I partly disagree

5. I disagree

64. "Human rights organisations are always entitled to be heard when important decisions on security and privacy are made"

1. I completely agree

2. I partly agree

3. I neither agree or disagree

4. I partly disagree

5. I disagree

65. "It is important that private companies involved in producing security technologies are also entitled to be heard when important decisions on security and privacy are made"

1. I completely agree

2. I partly agree

3. I neither agree or disagree

4. I partly disagree

5. I disagree

66. "In relation to significant decisions on the use of security technologies, it is imperative that alternative solutions are elucidated and included in the debate"

1. I completely agree

2. I partly agree

3. I neither agree or disagree

4. I partly disagree

5. I disagree

Proposals for privacy enhancing use of security technologies

In the following section we would like you to consider some possible proposals on how to implement, use and research in security technologies without infringing privacy. For every proposal we ask you to state the importance of carrying out the proposal.

- If you find it very important that the proposal is followed, circle 1 "Of high importance"
- If you find it important, but not top priority, you circle 2 "Of some importance"
- If you find that it is not very important, circle 3 "Of little importance"
- If you find that it is not important at all or the proposal should not be followed, circle 4 "Not important at all"
- If you are not sure what to answer, circle 5 "Don't know"

Proposals

67. Collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order

1. Of high importance

2. Of some importance

3. Of little importance

4. Not important at all

5. Don't know

68. Only authorized personnel can have access to collected personal data

1. Of high importance

2. Of some importance

3. Of little importance

4. Not important at all

5. Don't know

69. Prior to implementing, new security technologies must be checked for privacy impact

1. Of high importance

2. Of some importance

3. Of little importance

4. Not important at all

5. Don't know

70. Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts

1. Of high importance

2. Of some importance

3. Of little importance

4. Not important at all

5. Don't know

Final Questions

You have answered many diverse and detailed questions about security technologies and privacy. In conclusion we would like to ask you two final questions.

71. Have you changed your attitude towards security technologies in general in the course of completing this questionnaire?

1. Yes, my attitude towards security technologies in general has become more positive

2. Yes, my attitude towards security technologies in general has become more worried

3. No, I have not changed my attitude

4. Don't know

72. If there are any comments concerning security technologies that you would like to add or that you have not had the opportunity to express in this questionnaire, please feel free to make a remark below: *(open text box)*

1. I have nothing to add

2. Your remarks

_____

_____

_____

_____

_____

Chapter 2   Interview guidelines

Questions in bold must be discussed by the participants. Subsequent to every question is a short note on the purpose of the question. To most of the questions there are some subordinated questions. These subordinated questions are inspirational, and can be used to support the discussion if necessary. The subordinated questions do not have to be raised if it is not necessary to inspire the debate.

Interview questions

1. **What are your immediate thoughts about security technologies and privacy?**
   Purpose of the question: An open question to get the debate started and to give the participants the chance to present their immediate attitudes

2. **What do you think about the scenarios?**
   Purpose of the question: Make the participants talk about what they have read in the scenarios to get an idea of how their feel about the possible future presented within them

   Subordinated questions to inspire the debate – only if necessary:
   - How is the balance between security and privacy in the scenarios?
   - Do you think the benefits in the scenarios are important to achieve?
   - Do the scenarios draw a picture of an attractive future?

3. **What do you think are the important positive potentials of security technologies?**
   Purpose of the question: Make the participants focus on the positive potentials and get an impression of what they find is the most important gain of security technologies

   Subordinated questions to inspire the debate – only if necessary:
   - What can you gain with security technologies – try to give some examples?
   - What is the most important positive possibility?
   - Why is it important?

4. **What negative effects of security technologies are you worried about?**
   Purpose of the question: Make the participants focus on the negative side of security technologies, the threats, and get an impression of what they find is the biggest threat

   Subordinated questions to inspire the debate – only if necessary:
   - What are the negative effects of security technologies – try to give examples?
   - What is the most important negative effect of security technologies?
   - Why is it important

5. **When do you think security is more important than privacy – and opposite?**
    Purpose of the question: Make the participants debate the dilemma of security and privacy (the trade off) to get an impression of in which situations and how much privacy they will give up for security

    Subordinated questions to inspire the debate – only if necessary:
    - In which areas or situations do you find that it is okay for security technology to infringe privacy?
    - In which areas or situations do you find that privacy is more important than security?

6. **Who should be involved when deciding on implementing new security technologies?**
    Purpose of the question: To get the participants input on the democratic perspective and importance of involving different interest groups when deciding on implementing new security technologies

    Subordinated questions to inspire the debate – only if necessary:
    - Which interest groups should be heard? (Citizens in general, civil rights organizations, security technology developers, politicians etc.)

7. **Do you have any suggestions about the regulation of development and implementation of new security technologies?**
    Purpose of the question: To get the participants input on how to manage development and implementation of new security technologies

    Subordinated questions to inspire the debate – only if necessary:
    - Should there be any limitations on development of security technologies or should security technology companies develop anything they like?
    - Should governments implement every security technology they find important or should there be some regulations – and what regulations?

8. **Has your participation in today's event changed your attitude towards security technologies and privacy? If so: Why?**
    Purpose of the question: To find out if information and debate about security technologies and privacy have changed the participants attitudes toward the subject

9. **Do you have any final remarks, points or messages that you would like to ad? (take a round)**
    Purpose of the question: To give the participants a change to make a last statement before ending the interview meeting

    Subordinated questions to inspire the debate –only if necessary:
    - Have something made a special impression on you during the conversation?

Rules of thumb

"Rules of thumb" and tips on how to carry out the group interview in a good way.

Introduction

Start by presenting yourself, "My name is … I'm from …, and I'm going to be the moderator at this group conversation. But you just talk and I will make a list of speakers if necessary.

After that you do a presentation round where people say their name and why they have come to the interview meeting

After that the TAPE RECORDER IS STARTED !! This is done in a free-and-easy way and by a easy comment. It is important to create a light atmosphere and play down the seriousness to make sure that the participants are not oppressed by the situation.

The first question is raised and the group interview is on its way.

The first question is always a "brainstorm" question, and a can affect a lot of immediate attitudes. It is important to give space, be open and listen in the beginning.

On the way

It is not important that all participants answer all questions, but the interviewer should have an impression of what they all think.

If anyone is hiding, the interviewer can always ask "Do you agree, John, or what do you think?"

There will be overlap in questions and answers. Skip questions if they have already been debated and answered

Tick of on the way, when you think that a question have been debated

It is important that all questions are debated. But questions that are more important to the participants than the ones in the interview guide can appear in the discussion and there should always be time to discuss these questions (as long as they are related to the security and privacy debate).

If someone becomes too dominating, it is the interviewers' job to bring on the other participants. Ask e.g."What do the rest of you think?" Interrupt if necessary, it is important that everybody is heard.

If the participants don't say much at the group interview, the interviewer can "take a round" saying that "at the next question I would like to take a round where everybody gives an answer".

Ask for reasons and arguments, "How come you think that… / What is the reason for…

Be aware of the participants' reactions; do they feel comfortable, do they seem under pressure or uneasy etc.

If you are through all the questions before time, you can go back to some of the questions that have not been debated that much on the way.

Closing

When there is 7-8 minutes left, it is a good idea to take a round where everybody gets to make a final remark. The final remark can be things that they have not have the time to state already or points or messages they would like to underline.

You can also ask if something has made a special impression during the conversation.