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 5.2 Austrian report - Interview meeting about security technologies and privacy

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

Author(s): Johann Čas, Institute of Technology Assessment

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

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

This document describes the Austrian interview meeting and the results produced by this activity. The interview meetings are a core element of the participatory activities within the PRISE project involving citizens of six European countries. The Austrian interview meeting took place on the 12th of June in the premises of the Austrian Academy of Sciences, located in the centre of Vienna. It was organised and conducted by the Institute of Technology Assessment, the recruitment of citizens has been outsourced to a market research company. For more details on the venue see Annex 2 - Program of the interview meeting (in German only). No planned deviations from the procedures described in the method manual occurred apart from recruitment of citizens via phone instead by invitation letters.

However, a large number of cancellations on the last day before the event and unannounced non-appearance forced changes. Only 17 persons did actually show up at the interview meeting although 34 persons registered originally. Whereas the registered persons fitted very well to the selection matrix, in the actual group higher educated, elderly and female persons were over-represented. As a further consequence of the reduced number of participants, only three instead of originally planned four court interviews were conducted.

In the last two weeks before the interview meeting several short notices related to surveillance or terrorism were published in the press, however, none attracting large attention. Two contributions to TV magazines were also devoted to surveillance (development of surveillance after 9/11 in a political programme, costs of video surveillance in an economic magazine); both were broadcasted in late-night programmes with limited reach. The only event that attracted more attention - and that also was mentioned in the discussion - was the capture of the thefts of a Stradivari because of their fingerprints being stored in the asylum seekers fingerprint database.

Only little discussion took place in the plenum and the questions were focused on organisational aspects like the background of the project or the recruitment process. In addition, a suggestion also to take into consideration economic costs of security technologies was made.

Executive Summary

The general attitude of the Austrian participants could be summarised as "privacy aware and balanced against the benefits and threats of security technologies". Security technologies and measures are neither accepted nor rejected generally, but rather judged individually on a case-by-case basis.

The level of perceived privacy invasion is one decisive factor in this judgement. Video surveillance in public spaces is for instance regarded as much less privacy infringing than the combination and mining of different databases. The organisational setting and the legal framework for use and implementation of security technologies form a second important factor in this evaluation and the acceptance of such measures. An example for this category is the requirement of reasoned suspicion and of court orders for the implementation of surveillance measures or for the access to and personalisation of collected data. Further topics raised in this context were the wish to be informed about security technologies, their capabilities, and their actual uses as well as to have the individual choice to use or to activate personal security systems.

The perception of threats and the assessment of the contribution of security technologies to lessen these risks determine to a large extent the level of privacy invasiveness of certain technologies measures, that is regarded as acceptable. The Austrian participants differ considerably in balancing privacy against security; reflecting the different individual perceptions of risks, the willingness to accept them respectively to accept restrictions in privacy and human rights. A common bases within the Austrian participants is the need of proved security gains before accepting any privacy infringements, another one is the conception that a hundred per cent security can never be reached and therefore the proportionality of measures needs to be considered and proved in a proper way.

Austria has not suffered from any serious terrorist attack in the more recent past. Nevertheless, terrorism is regarded as an existing and inevitable risk for Austria too. The Austrian participants are however more concerned about crime and neighbourhood security and then about terrorism.

In general, the participants do not believe that security technologies can completely eliminate risks of crime or terrorism. The current level of attention to these threats is itself regarded as a potential threat to freedom and privacy. An atmosphere of fear may cause people to accept violations of privacy and civil freedoms that otherwise would be rejected.

A further prevailing tendency is a preference for alternative approaches and non-technical solutions. Alternative, less privacy infringing approaches should be applied wherever possible. One reason for non-technical solutions is that in person presence of security forces promises immediate assistance in the case of emergencies and more preventive power than surveillance technologies, which are assessed as being more helpful in the investigation and prosecution later on. Non-technical solutions to security problems include also the search for and fight against the roots of criminal and terrorist activities. Social, economic and political measures in these areas are regarded as more promising in the long term than the use of security technologies alone, which are not believed to be able to provide sufficient levels of security.

Whereas it was accepted that security technologies can certainly increase security, it was also believed that they can be defeated with enough criminal or terrorist energy.

The Austrian participants regarded their own involvement in the PRISE project activities as a very positive, but probably not very influencing experience. The democratically legitimised bodies should basically take responsibility, although there is some doubt to what extent they are acting in the public interest without being too much influenced by external economic and political interests. Hence public information and debate as well as the involvement of independent experts in decision-making is demanded.

Chapter 1 Participants general attitudes

Taking the statement “If you have nothing to hide, you don’t have to worry about security technologies that infringe your privacy” as indication of the general points of view, the majority of the Austrian participants can be characterised as privacy aware and having a deliberate position on security technologies and measures. Whereas no one completely agrees to this statement, 5 persons partly agree, 7 partly disagree and 5 persons completely disagree. This broad range of general attitudes, with a bias towards respecting the fundamental right of privacy, is also reflected in further statements related to general opinions.

To the statement “The security of society is absolutely dependent on the development and use of new security technologies” one person completely agrees, 5 persons partly agree, 7 partly disagree and 4 persons completely disagree. The answers to the question “Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror” show a very similar pattern with a slightly higher scepticisms about effectiveness and reasoning behind the implementation of security technologies (4 persons completely and 8 persons partly agreeing).

This range of attitudes also appeared during the discussions. Concerning video surveillance, a major topic discussed at the group interviews, the comments to the questions whether video surveillance makes oneself feel more safe or infringes his or her privacy reached from

> *No, not at all. Not at all. … The whole surveillance, the naked machine, I think it is a horror. I cannot feel comfortable there.*

to statements like

> *… basically I have nothing against surveillance.*

> *… I believe that surveillance is discouraging; … that people are saying we are not going to do it now, because we are not sure whether we are recorded or not …*

Although the participants had different positions they were in general aware of conflicting interests and accordingly discussing pro and cons in a thoughtful and open way.

The answers to the statement “When security technology is available, we might just as well make use of it” provides further evidence for the differentiated perspectives of the Austrian participants. Five persons agree (1 completely and 4 partly), two are indifferent and 10 disagree (5 each completely and partly); hence for a majority the availability is not a sufficient condition for the use of particular technologies.

Among the general questions about security technology and privacy the statement “Privacy should not be violated without reasonable suspicion of criminal intent” received the most unambiguous response: 15 out of 17 persons completely agreed, 1 partly agreed and 1 partly disagreed. A very clear indication that acceptance of surveillance measures is bound to specific conditions. In the group interviews this line of argumentation came up in different forms, e.g. a requested need of effectiveness or court orders before certain measures can be taken.

A vast majority (7 persons completely and 7 partly) agreed to the question “It is uncomfortable to be under surveillance, even though you have no criminal intent”. The dominant emotional discomfort of the Austrian participants is substantiated by the fact that no one completely disagrees to this statement.

Regarding the likelihood of abuse of security technologies the vast majority (about 90%) of the participants believes that there is a chance that these technologies will be abused by governmental agencies (16 out of 17) or by criminals (15 out of 17), meaning that only 1 respectively 2 persons completely disagree. The participants were however more uncertain about abuse by governmental agencies (3 persons completely agreed) than about abuse by criminals (9 persons completely agreed).

In the group interviews the participants showed often a tendency to listen to opposite opinions and to adjust their judgements from rather extreme to more moderate positions; security technology sceptic persons accepted that these technologies may make life more secure, technology affinitive persons acknowledged that security gains may not justify losses in privacy linked to the use of certain security technologies.

Several persons doubted the effectiveness of technical solutions, and in some cases the objective to increase security in general.

> *I think, they don't discourage anyone, if someone wants to take it [a bomb] with him*
>
> *I think,, if you cannot find measures against such things [youth criminality] in advance, surveillance cameras will not be of much help in the end.*

Insecurity or risk is accordingly regarded as an inescapable part of living. These persons were not willed to exchange small gains in security for losses in freedom and privacy. Nevertheless, there was hardly any fundamental rejection of security technologies in general and for all possible uses. The acceptance was, however, bound to certain conditions like the proved effectiveness in the particular use case, the presence of reasoned suspicion or the involvement of judges in decisions on the use of these technologies and of the generated data.

Several statements were related to the relation people versus technology, e.g. whether more police forces or more technology is more effective.

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

Another attitude shared by many participants was the persuasion of the impossibility to defeat terrorism by technical means unless efforts focus at the roots and reasons of terrorist activities.

The majority of the participants have not changed their opinion when filling the questionnaire (14 out of 17), the remaining persons got a more positive attitude. At the end of the group discussions the participants answered a similar question orally in a more differentiated manner: although again a majority reported no general change in their attitudes towards security technologies, the information provided and the discussions were regarded as an important contribution to a more profound knowledge and awareness about security technologies.

Chapter 2 Security technologies

2.1 Biometrics

Concerning using biometrics for access control about one third of the participants will not feel comfortable using any kind of biometrics (6 out of 17). The rest feels more comfortable using fingerprints than facial or iris recognition (9, 5 and 4 out of 17 feel comfortable).

When the location where biometrics are applied respectively the purpose of the use of biometrics is the differentiating factor, then only 3 out of 17 persons cannot accept using biometrics at all. The highest acceptance occurs for airports (12), banks (7) and border control (6), while biometrics in bus and train stations, private services and stores (3, 2, 1 out of 17) are the least of all accepted applications.

Biometrics possess the highest degree of acceptance in airports, the predominant part of the participants feels, however, insecure using the biometric passport because of the risk of biometric data being stolen.

When the registration of biometric data in a central database as a step to fight crime is questioned whether it is acceptable, the participating citizens are divided into to even groups (7 agree, 2 NN, 7 disagree).

2.2 Camera Surveillance

Camera surveillance, as an application most persons are already confronted with in daily life, was also in Austria the most discussed technology in the group interviews.

The answers show that there is a relatively high degree of acceptance of camera surveillance. About 2/3 of the responding participants think there is either an appropriate number of surveillance cameras in the society in general or that there should more cameras (11 appropriate and only 1 wanting more). Most of the participants can accept it in banks (15 out of 16) and in airports (14), camera surveillance also gets relatively high acceptance in sports arenas and other crowded areas (9), in bus and train stations (8) and in stores (7). However, only a quarter of the participants can accept surveillance in all public places (4 out of 16) and only 1 in dressing rooms to prevent theft.

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

A slight majority feels more secure under video surveillance (3 persons completely and 6 partly agree out of 17), about one quarter (4) does, however, completely disagree. A majority also regards camera surveillance as privacy infringing (3 persons completely and 7 partly agree), 5 persons disagree to this statement (1 person completely and 4 partly).

Several aspects of video surveillance were raised during the group discussions: e.g. effects on perceived and actual security, or alternative solutions. Quite different personal opinions about the impact of video surveillance on feeling personally more secure were brought up. Main lines of argumentation behind these different assessments were varying judgements of preventive versus investigative functions of video surveillance and the occurrence of net positive effects on crime rates or just shifts to unobserved places.

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

In general, some positive effects were acknowledged but different opinions about the proportionality of video surveillance prevailed. Some persons strongly favoured more presence of police forces to technologies.

The differences between passive or active cameras were not explicitly discussed. However, passive cameras were largely accepted as long as the duration of storage is strictly limited and clear rules for access to recordings exist. From a security perspective active cameras were preferred as in these cases immediate assistance in case of threats or emergencies is possible.

2.3 Scanning

"Where is scanning of persons for detection of hidden items necessary for security reasons?" Answering this question one quarter of the responding participants (4 out of 16) find scanning for no reason acceptable; the same number of person (4 out of 17) accept no type of scanning. Acceptance is highest in airports (13 out of 16), all other locations receive low acceptance (3 each for schools and central bus and train stations or complete disagreement (shopping malls). The only method a majority can accept is scanning for metal objects (10 out of 17), the real naked machine and scanning of body heat, sweat and heart rate are not at all accepted. A majority disagrees (5 partly, 5 completely) that scanning is an acceptable tool for prevention of terror.

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

2.4 Locating technologies

Locating of mobile phones and locating of cars is acceptable for a majority of the participants, as long at the location is either based on a court order (13/12 respectively for mobile phones/cars), connected to an accident (14) or with the purpose of locating a stolen car (12), meaning that all these uses are accepted by approximately 3/4 of the participants. However, the court order is the decisive factor for the Austrian participants, locating of suspects without a legislative command is regarded as not at all acceptable.

A vast majority of 15 out of 16 find using eCall for speeding control and automatically giving of speeding tickets unacceptable, about three quarters find it acceptable for locating stolen cars or automated accident reporting. The predominant part of the participants think that installing of eCall in new cars should either be optional or it should be possible to deactivate this function (9 respectively 6 out of 16).

> *As a citizen I have the right to vigilantness.*

The predominant majority of the participants finds both the possibility of locating cars and mobile phones privacy infringing. Regarding the question whether they are a good tool for the police for the investigation and prevention of crime and terror, the picture is more differentiated: 12 persons agree (5 completely, 7 partly) for mobile phones, for cars only 6 persons agree (1 completely, 5 partly).

2.5 Data retention

Data retention is acceptable for a majority of the participants as long as the purpose is investigation of specific terrorist attacks (10 out of 17) or crimes (9 out of 17) that have occurred. When it comes to prevention only a minority of the participants can accept the use of stored data, 6 out of 17 in both cases. Similar answers were given for the scanning and combining of personal data from different databases. Four persons find data retention never acceptable, 2 the scanning and combining of personal data from different databases.

A majority of the participants (8 out of 17 completely, 6 partly agree) also finds scanning of personal data privacy infringing and states that traffic data from communication should not be stored for purposes apart from billing (11 out of 17 completely, 4 partly agree). Moreover 16 out of 17 participants state that function creep is a serious privacy problem.

On the other hand, more than the half of the participants (3 completely and 6 partly agree out of 17) think that scanning and combining of personal data is a good tool for the police to prevent terror.

It is noticeable that 4 out of 17 participants indicate that data retention, and 2 out of 17 that scanning and combining of personal data from different databases is never acceptable. A majority finds it unacceptable for governmental institutions to store all data they find necessary for security reasons. This suggests paying more attention to the privacy problems of data retention.

2.6 Eavesdropping

Similar to locating technologies, the court order is also the decisive factor concerning eavesdropping. A broad majority can accept eavesdropping as a mean of prevention and investigation of both crime (15 out of 17) and terror (13 out of 17) as long as there is a court order authorising it, while only 1 out of 17 also accept it without a court order in both cases. A majority finds eavesdropping privacy infringing, a tight minority also to be a good tool for police investigation.

Eavesdropping of a suspect is the most acceptable method (8 out of 17) while only a minority can accept eavesdropping of persons that suspects are expected to contact (6 participants), no one accepts general eavesdropping of all communication lines and 2 participants find eavesdropping never acceptable.

2.7 Privacy Enhancing technologies

13 out of 15 answering participants agree that Privacy Enhancing Technologies (PETs) are a necessity in today’s society to preserve privacy (7 completely and 6 partly), 2 neither agree nor disagree. When asked what technologies they think should be accessible 2 participants answered that they don’t know and 2 did not answer at all. This probably indicates a large degree of insecurity or lack of knowledge towards these technologies The most preferred PETs are encryption programmes (11 participants) and anonymous calling cards (10 participants) followed by identity management (8 participants). A majority disagrees to the statement “Privacy enhancing technologies should not be legal if they make police investigation and

prevention of terror and crime more difficult" (7 completely and 3 partly), 5 person agree to it (1 completely and 4 partly).

2.8 General attitudes

Video surveillance, as a very present technology was a main focus of discussions in the group interviews. As long as this surveillance is taking in public places there was a rather high degree of acceptance as long as storage and access to recordings are limited and regulated; moving in public space was in general linked to a low level of privacy. The distinction between passive and active cameras did not seem to play an important role in the general acceptance of video surveillance; active systems were rather preferred as they increase the chance of in time intervention in the case of emergencies.

Access to and combining data from different sources were the most strongly disaffirmed security technology application. Here the potential abuse for commercial purposes or political control of the citizens appears to be the main reason for the broad rejection.

> *I regard video surveillance, where the data are deleted within 48 hours if nothing happens rather justifiable than the request to provide personal identification for every bit …*
>
> *… combining personal data … here I would rather flinch, then for a camera that watches some dark corner.*

Doubts were also raised about the effectiveness of security technologies because of the skills of criminals or terrorists.

> *… all those terrorists and so, they are so clever, they grasp the technologies in a short time and then the whole thing becomes useless..*

More general comments requested to focus on the roots of security threats instead of concentrating on technical solutions.

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

Chapter 3 Dilemmas of security and privacy

3.1 Convenience when travelling

The first dilemma the participants were confronted with was convenience when travelling, taking easy payment in the underground based on using fingerprints for registration and access to public transport. Almost all of them are not willing to accept this privacy infringement for the convenience of easy payment (16 out of 17 participants), 4 participants indicate that they could accept it if it is optional to use fingerprint and not the only possibility. Convenience when travelling in public transport is definitely not more important than privacy for the vast majority of the Austrian participants.

> *… fingerprints, where you feel like a criminal …*

> *… ok, as internal security technology in companies, but for train tickets …*

When travelling by plane is concerned the participants are a bit more willing to accept losses of privacy for convenience. About two thirds of the participants (11 out of 17) cannot accept any loss of privacy for fast and convenient check-in. Five of them can accept some privacy infringing security technologies; the technologies and means are thorough pre-registration and use of biometrics and going through the naked machine. Being scanned for sweat, body heat and heart rate is unacceptable for the Austrian participants.

3.2 Prevention of terror

The dilemma of prevention of terror contra privacy is perceived as difficult by the Austrian participants. Active surveillance cameras and automatic face recognition (AFR) in airports and train stations could prevent terrorist attacks, but they could also lead to that innocent persons are mistaken for terrorist and taken aside for questioning. The participants are divided in this dilemma. 4 participants think that active cameras and AFR should not be used at all, 6 participants think that the technologies should only be put to use if no one is mistaken for terrorist and 5 can only accept a low rate of people are wrongly taken as terrorists. None of the Austrian participants agrees to the question "Active cameras and automatic face recognition should be used no matter how many innocent persons are mistaken for terrorists". A majority of the participants can accept this kind of surveillance in places that are very vulnerable to terror or where many crimes have occurred.

> *No, I don't think that these criminals possess an inhibition level. But I'm not generally against surveillance because I think it may discourage the one on the other …*

Some participants disagreed to accept privacy infringements in exchange for security gains.

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

Another technology that is supposed to be useful in the prevention of terror is scanning and combining of data from different databases with personal information in order to detect suspicious patterns. Anonymous collection and only a court order can have the identity revealed are here the decisive factors: in this case 13 out of 17 persons can accept this measure; 4 can never accept it and only 1 participant can accept these measures without any restrictions.

The possibility of function creep and abuse are important factors in the perception of dilemmas of security technologies and privacy.

> *Definitely. Abuse is written in big letters above it. Above each advantage.*

3.3 Locating of cars and movements

The eCall technology can register the movement of cars. These records can be used for different purposes and with different degrees of privacy infringements. 5 out of 17 participants can accept that eCall is used for the original purpose, which is registration and reporting of the cars position in the case of accidents, 7 can accept that police can activate the eCall system and locate a car to prevent crime or terror. At the same time the majority of the participants (12 out of 17) think that installing of eCall must be optional and only one person wants the system to be used for issuing speeding tickets. None of the Austrian participants accepts that the movements of his/her car are registered at all times. This indicates that the participants primarily want the eCall system to be used for the original purpose and that they don’t want any kind of “function creep” in the use of the technology, with a bit less than the half of participants accepting the exception of prevention of crime end terror.

In the discussion affected and non-affected persons were distinguished:

> *When I have an accident, …, when I’m affected, I will be very pleased if assistance arrives as soon as possible … if my car is stolen, I would be very happy if I could go to the police and to tell them: “Please switch it on and look, were my car is!” This will always be the case if I am affected.*

3.4 Privacy enhancing technologies for all

Privacy enhancing technologies can be used by ordinary people to protect their privacy, e.g. when communicating or using the internet. But these technologies can also be used by criminals and terrorist and might make police investigation and prevention of terror and crime more difficult. The predominant part of the participants are willing to accept legal anonymous calling cards (13 out of 17), a majority the legal use of encryption (9) even though it might make police investigation and prevention of terror and crime more difficult. Concerning the anonymity when using the internet, the picture becomes more complex. When the consequence is that persons searching for bomb instructions cannot be traced by police a tight minority of the participants (8 out of 17) can accept internet anonymity, this number is reduced to 5 participants when the consequence is that persons searching for child pornography can not be traced by the police. Privacy enhancing technologies are important for the majority of the participants; only 4 participants cannot accept any PETs that might make police investigation and prevention of terror and crime more difficult.

3.5 Consequences for others

The last dilemma the participants were confronted with was what consequences they would accept for other people if a security technology could provide great security enhancements. The consequences taken as example where exclusions from public services or troubles using public transport. The predominant part of the participants is not willing to accept any consequences for neither people who are not able to use a certain technology (e.g. absence of useable fingerprints) nor for people who don’t want to use it for privacy reasons (11 participants each). Regarding the acceptance of some consequences there is a slight difference between people unable to use technology and people unwilling to use the technology. The respective rate increases from 2 to 3 for public services and from 1 to 2 for public transport.

Chapter 4 Democratic issues

4.1 Democracy and participation

The discussion on democratic aspects of decision making on security technologies was characterised by a broad range of different opinions and individual uncertainties about in which way and to what extent to involve public participation. Whereas during the discussions there was a rather broad agreement that the elected government should be the main responsible body, many participants also expressed doubts about the independence and competence of politicians to make decisions in the best public interest. Specific doubts that were mentioned concerned the influence of economic interests of the security industry and of foreign countries, particularly of the United States on European policy.

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

> … *since the attacks in America these things are strongly pushed my America.*

The involvement of independent experts in the decision-making process was also discussed to some extent; some participants raised doubts about the possibility to find really independent experts.

More and stronger public participation was regarded as generally very important.

> *If my privacy is affected, I must be asked in any case ….*

All participants agreed that politicians must always submit important questions to public debate and public hearings before making decisions (70 per cent completely agreed, 30% partly). A few participants regarded the issue as too complicated for inclusion of the general public in decision-making (1 completely and 3 participants partly agreed to this statement).

The participation of human rights organisations in decision-making on security and privacy also received a very broad acceptance (13 out 17 participants completely agreed, 4 partly). The involvement of private companies was also regarded as important, however, with a less clear voting (about two thirds completely agreed, the rest was uncertain or disagreed).

All participants agreed that alternative solutions should be included in the debate (16 out of 17 completely agreed to this statement). This result is also supported by several contributions to the discussion in which alternative solutions were proposed, e.g. more presence of policy forces instead of surveillance by technology or more focus on measures against the reasons for crime or terrorism.

4.2 Proposals for privacy compliant use of security technologies

At the end for the questionnaire the participants where asked to evaluate the importance of four proposals for privacy compliant or enhancing use of security technologies. The proposals were evaluated as shown in the following table.

Proposal	High import.	Some import.	Little import.	Non import.	Don’t know
Collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order	17	0	0	0	0
Only authorized personnel shall have access to collected personal data	17	0	0	0	0
Prior to implementing, new security technologies must be checked for privacy impact	15	1	0	0	1
Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts	14	1	2	0	0

The proposals were generally ranked as very important by the Austrian participants. Specifically the first two proposals on the regulatory and procedural aspects of collection and access to personal and received an unanimous voting of high importance. This result confirms the broad rejection of surveillance of unsuspicious individuals within the Austrian group of participants.

The next two proposals, concerning the research on and the implementation of new security technologies were also regarded as very important, but to a slightly less unequivocal degree. Explanations for this could be some mistrust in the effectiveness of such measures and in the neutrality of the involved organisation.

Chapter 5 Additional information

5.1 Opinion of the participants on the event

The reactions of the participants on the event were very positive. On the one hand, they stated that the information provided and the discussions have increased their knowledge and raised awareness of societal issues related to security technologies. In general, this event did not change their attitudes towards securing the technologies, but enabled them to discuss and the thing about these issues on a more profound basis.

The participants also appreciated very much that they had been given the opportunity to express their opinion on these issues and to get involved in decision-making. They were however also concerned about the real impact of this event and expressed the wish that public participation should become a regular part of decision-making on technologies that impact their daily life.

5.2 Additional aspects discussed by the participants

During the event the participants took new perspectives and raised questions that were not covered by the questionnaire and interview guidelines.

One issue that was addressed in the discussions concerned the relation between security technologies on the one hand and the general trend towards a surveillance state, on the other hand. The promotion of security technology was regarded as an intended and planned political tendency aiming at transparent citizens.

> *I have the impression that this is a definitely wanted development, wanted politically or by the government. … an as much as possible complete identification;. the transparent citizen so to say. And this is done in a piecemeal, systematic way.*

Some participants shared the impression, that extreme situations and fear are abused to implement more surveillance technologies.

> *... but it are always borderline situation, and they serve as reason for general measures …*
>
> *There always will be some persons, who have been made afraid enough to vote for more surveillance.*

Another new aspect that was raised concerned the health impacts of the radiation used for advanced body scanners like the naked machine. Some participants claimed that these impacts need to be investigated in detail, specifically for frequent travellers, to avoid possible long-term negative health consequences.

Further aspects addressed in the discussions, but not discussed in detail included information security aspects, specifically when using the Internet, the security of RFIDs used for biometric passports and the definition of terrorism respectively the danger of abusing this definition for the discrimination of politically critical groups.

Overview of Annexes

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

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