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 5.4 German Report
Interview meeting about security technology and privacy

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

Author(s):
Maren Raguse, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Revision 1

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

Following the methodology laid down in the PRISE deliverable D 1.3 'Interview Meeting Manual' the objective of the German national interview meeting was to determine the participants' view on the questions relating to privacy and inner security measures and technologies and the balance between these two.

The German interview meeting was held on 15 June 2007 in conference facilities of the Kiel Chamber of Commerce. The event was organized by Kai Janneck and Maren Raguse of ULD who were supported during the meeting by Dr. Moritz Karg and Christian Krause. The team of organizers was chosen with regards to their different scientific background, including business administration, law and social sciences, in order to allow a multi-disciplinary approach to the realization of the interview meeting. For ULD, being a supervisory data protection authority[1], the interview meeting approach chosen as the participatory element of PRISE was as yet new.

In order to allow comparability of the six European events, close observation of the proceedings for preparation and conduct as laid down in the method manual provided by DBT were regarded essential by ULD. However, during the invitation process, ULD – due to its position as a public authority responsible for supervision of data protection compliance in the German state of Schleswig-Holstein – had to refrain from using all of the suggested methods for recruiting participants for the interview meeting and did, in order to compensate for the possible lower number of replies, turn to the following additional methods to recruit participants for the interview meeting.

The method for recruitment of participants suggested by DBT did comprise a three-step approach:

- 1st step: mailing of 2.000 invitation letters to random addressees.
- 2nd step (if step 1 does not return enough registrations): call citizens chosen at random and invite them.
- 3rd step (explicitly only a fallback option, if the aforementioned steps should not return enough registrations): nominate participants in personal / business network.

ULD, when supervising compliance with data protection requirements in the private sector, is regularly approached with complaints about soliciting calls from companies which by citizens are frequently perceived to be intrusive and disturbing. In addition, German law prohibits specific means of contacting individuals via telephone and e-mail. Even though the Unfair Competition Act[2] does not apply to a situation where a research project is looking for participants to an interview meeting[3], ULD feels committed to the general view behind the Act

[1] See Article 28 of Directive 1995/46/EC.

[2] Gesetz gegen den unlauteren Wettbewerb (UWG).

[3] The Act aims to prevent certain trade practices which are considered to be unfair. The Act covers actions by market participants – competitors, consumers and the general public – which aim to increase the sale or supply of goods or services.

and considers unexpected telephone calls to be intrusive for the callee and thus incompatible with ULD policies. For this reason it was important for ULD to recruit enough participants by means of approaching them in writing (step 1).

When looking for possible means of acquiring 2.000 random addresses, ULD's options again were restricted by its official position. It is possible to buy addresses from address-sellers who aggregate address databases from publicly available sources such as telephone books. A second source for the addresses sold by address-sellers is a broad range of companies who sell their customers' addresses. German law regulates an opt-out provision for data subjects who do not wish to receive advertisement by ordinary mail. As it is not sure to what extend all sources of address-sellers inform their customers of this right to object ULD decided to follow a different approach and extracted the 2.000 addresses from the public phone directory. 22 out of the 2.000 letters were undeliverable and were returned to ULD with an according note.

Sending out the first round of invitation letters (2.000) did return only 17 registrations within the deadline for replies (14 May 2007). The method of approaching another 2.000 citizens with a written invitation was not considered effective taking into account the comparatively small number of replies in relation to the mailing costs for 2.000 invitations. In order to reach a broad range of citizens with different background and no prior knowledge in the field of privacy or inner security, ULD placed a newspaper advertisement in a local newspaper. Additionally, as the first round of invitations returned replies mainly by citizens with higher or medium education, flyers were put up at a local vocational school.

The invitation letters were sent only to citizens listed in the phone directory for Kiel. The newspaper advertisement appeared in a newspaper called 'Kieler Express'. The newspaper has a bi-weekly edition of 242.770 copies and is distributed within a distance of 50 kilometres north, 43 kilometres west, 26 kilometres south and 41 kilometres west of Kiel.[4] As a result, three of the registered participant came from outside Kiel and the rest from Kiel.

Finally, these means returned 31 registrations altogether. Of these 31 registered citizens no one was rejected as no apparent prior knowledge in the discussed topics was to be concluded from the professions stated on the registration forms.

On the actual day of the interview-meeting, not all of the registered participants did show up, the majority of them without giving a reason. Out of the 31 expected citizens only 21 (67,74 %) came to the venue on the day of the interview meeting. A drop-out rate of 32,26 % was unexptectedly high. The two participants who announced in advance of the meeting that they could not participate gave two different reasons: prioritized private appointment and sickness. A third participant called after the meeting, explaining that she simply forgot about the meeting.

The recruitment and preparation process was carried out between 2 May and 25 May. The timeline of the invitation process was the following:

- 7 May 2007: mailing of 2.000 invitation letters

[4] The area of circulation can be found here (p. 8): http://www.kn-online.de/kn-anzeigen/preise/KE.pdf.

- 19 May 2007: newspaper invitation via advertisement
- 14 May 2007: Flyer Vocational School
- 22 May 2007: pilot test questionnaire
- 25 May 2007: sending out 31 confirmation letters (with Scenarios)
- 15 June 2007: date of interview meeting

Feedback given after the pilot test was that the questionnaire was perceived to be too complex by the low educated test candidate.

The chosen venue for the interview meeting, the Kiel Chamber of Commerce, provides conference rooms of different sizes, suitable for the group discussions as well as the joint part of the interview meeting.

The interview-meeting progressed as scheduled in D 1.3. After an introduction into the dilemmas between privacy and inner security by Maren Raguse from ULD (30 minutes), the participants raised questions. Then the questionnaires were handed out. Very few questions were asked during filling out the questionnaire (50 minutes). The participants were divided into 4 groups. The groups were divided based on an equal division of age and sex. As all registered participants with low educational background had not shown up and due to the high drop-out rate, the grouping made prior to the event based on the registrations was impossible to keep up. A new grouping adjusted to the actual participants was carried out while the participants were filling out the questionnaire. Afterwards, the participants went to different rooms where the group interviews were carried out (1 hour).

The interviews were recorded on tape and transcribed. The recording was deleted after the transcription process.

Executive Summary

The level of acceptance of security technology is closely interlinked with the intended purpose of use and the site where the technology was going to be applied. Especially with regards to transportation and airport, citizens tend to accept surveillance and use of security technologies

The majority of participants is generally willing to give up some of their privacy, depending on the circumstances. Many of them called for the government deciding on security technology implementation to give them a choice about using it. A privacy conscious and self-determined state of mind should not lead to negative consequences for individuals exercising what seems to be perceived a general right – the right to give or not give up privacy.

Participants were split in three groups, ‘the privacy advocate or sensitized participant’, ‘the undecided participant’ and ‘the security advocate’. Most participants feel uncomfortable when being under surveillance. Yet, many acknowledge that developing new security technologies is essential for the security of the state.

The effectiveness of security technologies plays an important role for its acceptance. Not only do citizens insist that alternative measures should always be considered; these could be less intrusive or/and more effective and thus foster proportionality of use. Also it must be stated that even if a security technology is perceived to be effective, it may still lack acceptance among citizens because it is considered to be too excessive. This position was predominant with regards to data retention.

The interviewees reject data collection which is conducted regardless of whether they are suspected of any wrongdoing. Measures not based on a concrete suspicion just like very intrusive security technologies use are only accepted if based on a court order.

In general, if measures lack transparency only citizens with a very high level of trust in the government do still support these. In this context, building central databases and combination of data from different databases received low acceptance.

Citizens call upon their government to get a say in the debate about the introduction of security technologies, even if questions regarding these technologies may be complex. An evaluation of alternatives and the effectiveness, involving experts, manufacturers and Human Rights Organisations found broad support.

Chapter 1 General attitudes

In Germany a public discussion has been going on for several months centring on the question whether and which kind of new security measures and in particular new law enforcement powers should be implemented in national law. In this context broadcasting and / or newspaper articles dealing with security measures and their possible impact on society as well as their possible effectiveness have been available. Many participants' awareness seemed to have been fuelled, if not raised, by this ongoing discussion. This can be concluded from the group interviews which all at some point dealt with some of these proposed measures. Some participants, when registering for the meeting, explicitly explained that the current discussion on new security measures and their concern for privacy implications in this context were the driver for them to come to the meeting.

The participating citizens voiced very diverse opinions and statements during the group discussions and when filling out the questionnaire. The citizens present shared the common view that privacy should only be infringed based on a reasonable suspicion of criminal intent. All participants agreed that some use of security technology is necessary but opinions on the balance of privacy infringement and extend and effectiveness of security measures varied greatly.

Abstracting, the citizens present can be divided into three general groups regarding their general attitude towards the dilemmas and questions discussed:

- 'the privacy advocate or sensitized participant': weighs privacy to be an important right and is largely concerned by use of security technologies. Some participants endorsed an exaggerated idea of what is actually lawful or being carried out by German law enforcement and intelligence. In this group the apprehension was stated that Germany was moving towards a surveillance society. Also there was a dominating general distrust in public authorities and government.

- 'the undecided participant': does not perceive privacy infringement to be a substantial problem in his life but still does not support extensive surveillance measures or use of security technologies.

- 'the security advocate': does not perceive surveillance and security measures to be uncomfortable and supports the intended gain in security. Only very few participants fully supported this position and agreed to the statement 'I have nothing to hide and therefore don't mind surveillance or other such measures.' This group generally trusted governmental activities.

In this context it can be stated that the female participants of the interview meeting overall can be matched mainly to the group 'the privacy advocate or sensitized participant' as well as the 'undecided participant'. 'The security advocate' at this meeting was represented only by male participants.

As far as age as a determining factor for the mind-set is concerned, young participants tended to be rather sceptical, if not troubled by extensive use of security technologies while participants of the group '55+' were predominantly supporting the view that the security of the society is absolutely dependent on the development and use of new security technologies. A feeling of mistrust towards the state was described by some participants to be the result of the introduction of new security technologies:

> *Looking at myself I can state that my attitude towards security technologies has changed profoundly during the past ten years. Some ten years ago I would have said 'I am a respectable citizens and I will probably never commit a serious crime. What could they pin on me? What do I have to hide?' But the more security technologies are being introduced, the more I am opposing this trend.*

Yet, age did not on all questions return such evident differences in opinion as the vast majority of participating citizens partly or completely held the view that many security technologies are not effective regarding an actual increase of security but are only being applied to show that something is done to fight terror. Age did not make a difference on the mindset regarding this question.

Surprisingly, bearing the citizens' aforementioned general position in mind, age did play a role concerning the opinion on whether all available security technologies should be made use of. Only participants older than 55 could completely agree to this statement, and the majority of participants older than 55 partly or completely agreed to this view.

> *I have come to realize that life has changed within the past 40 years. And if the people do assign the mandate to the state to provide security – then I expect that all technologies are used which can protect us.*

Contrary, the majority of participants aged 18 to 49 partly or completely disagreed to a self-evident use of available security technologies.

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

The current development of steady extension of security technology use was strongly perceived to be a one way spiral with no consideration of when and what kind of extended powers could be decreased in the foreseeable future:

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

A strong concern about a lack of transparency regarding what kind of data is collected about citizens at which occasion was voiced especially by the 'privacy advocate or sensitized participants'. This concern was associated with a feeling of discomfort related to uncertain impression that data from different sources will be linked without any knowledge or transparency for citizens. In addition to that, a majority of participants feared abuse of security technologies by governmental agencies and all participants – fully or partly – expect misuse of new security technologies by criminals.

But, depending on the situation a technology is used in, most citizens named specific use cases where they explained that the use of security technologies would lead to a feeling of security.

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

All citizens who decided to come to the interview meeting were particularly interested in the topics signalized by the invitation letter and the scenarios sent out prior to the meeting. Many of the participants discussed the issues at question based on personal encounters and experiences. They perceived the interview meeting as a possibility both to have a say and to learn from the discussions scheduled. The participants seized the chance to find out more about the currently discussed approaches of extending law enforcement authorities' power of intervention and asked according questions after the introductory presentation.

Chapter 2 Security technologies

The interview meeting and especially the group interviews revealed very diverse opinions among the participants regarding individual security technologies. Most participants mentioned that the interview meeting and the distributed supporting documents (scenarios and questionnaire with info boxes) provided new knowledge to them on previously unknown technologies. As far as specific security technologies are concerned, the group interviews centred on

- ‘common’ security technologies like CCTV with which the participants had been in contact with in their everyday life,

- technologies which had been previously unknown to the participants or of which they had only vaguely heard but whose privacy implications were perceived to be exceptionally strong by the participants.

2.1 Biometrics

The acceptance among participants varied depending on the specific kind and purpose of biometric systems. The majority of the participating citizens oppose the use of biometrics for access control and do not feel comfortable when using any of the three characteristics face, fingerprints or iris for this purpose. Even though averagely ¾ of the participants rejected using face, fingerprints or iris – the most common biometric characteristics – only half of the participants stated that they felt uncomfortable using any biometrics for access control.

With regards to implementation of biometric access control in particular places acceptance among the participants varied. More than half of the citizens can accept biometric access control at airports and almost half of them at borders. For other use cases, acceptance was lower. Especially the use of biometric access control in stores or for other private services was strongly rejected. But also use of biometric access control in banks, central bus stations and train stations as well as in stadiums and other crowded places was supported by only ¼ of the participants. With regards to biometrics, one participant voiced his opinion:

> *I would not only ask if it is possible, but what I would like to know if the data is needed, if these patterns are needed; if fingerprints are stored, and then you have to spend even more money to make sure no one can break the technology, I think you should at first ask for a purpose - why we have to give away this data.*

For 2/3 of the citizens a feeling of discomfort is associated with using the biometric passport as they fully or partly fear the risk of their biometric data being stolen. Yet in one group interviews all interviewees explained they had never before heard of a possible misuse of biometric data and could not imagine how such a misuse might look like.

Very different opinion among the participants existed with regards to the implementation of a central database with biometric data (for example fingerprints or DNA). More than ¼ of the citizens fully or to some extend consider storing biometric data of all citizens in a central database an acceptable step to fight crime. Yet, almost 60 percent completely disagreed with this approach being an acceptable step to fight crime.

2.2 Camera Surveillance

Also with regards to the use of CCTV the opinions and level of acceptance were very diverse. The level of acceptance was greatly depending on the specific use case. While none of the participants could accept the use of CCTV in dressing rooms in order to prevent shop lifting, the perception of privacy invasion in relation to security gain was nuanced for other use cases. Surprisingly, more than 60 percent of the participating citizens opposed one of the most common scenarios of CCTV implementation: monitoring shops with video cameras is not welcomed by the majority of the present customers.

The opinion on whether CCTV violates privacy varied greatly. 2/3 of the invited participants fully or to some extend held the view that privacy infringes their privacy. On the other hand 30 percent completely or partly disagreed with this position.

Video surveillance at banks, airports and stadiums received a high level of acceptance (between 60 and 76 percent). It can be concluded that the participants apply a simple rule: the higher the apprehended abstract risk associated with a certain kind of site, the more acceptance is stated regarding CCTV at that site. Consequently, the vast majority of citizens object to video surveillance in all public spaces and on the other hand only one citizen stated he could never accept video surveillance, no matter the circumstances. Even though 80 percent do not support CCTV in all public spaces, only ¼ of the participants think there should be no video cameras in public spaces at all. Almost 30 percent consider the number of existing cameras in public spaces to be appropriate, while 14 percent call for less and 10 percent for more cameras.

The effectiveness of active and passive CCTV was discussed intensively by all groups as CCTV seems to be a security technology all participants have been in contact with. While 60 percent of the participants explained that CCTV provides a feeling of security to them it was also stated that this feeling of security lasted only as long as they imagined that the CCTV system was an active system with security personnel monitoring events in real time. Passive CCTV in that context was regarded to bring about a deterrence effect as long as no public knowledge about the specific type of video surveillance implemented existed. Neither passive nor active CCTV in the eyes of some participants presents an effective means to prevent crime; passive CCTV was regarded to be not effective because no instant response by security personnel is possible due to the general design of the system. But even active CCTV was not regarded effective for crime prevention, only for prosecution as in the event of a crime, response would take too much time.

> *The problem is that even if you put up more and more cameras you will not have enough personnel to watch them all, and people know that. So I think it is a kind of pseudo-security.*
>
> *Yes, but it gives the opportunity to determine the perpetrator afterwards, even if you cannot prevent the crime.*

The use of active cameras and automatic face recognition (AFR) was controversial among the participants. Only one participant considered it acceptable to use active cameras and automatic face recognition no matter how many innocent persons are mistaken for terrorists. A second participant would accept the use of AFR if only low rates of false positives turned out. 1/3 of the citizens oppose AFR under all circumstances, even if it returned no false positives. Almost 50 percent would accept the use of AFR if it returned no false positives. With regards to the site where AFR could be implemented, more than 40 percent of the participating citizens could accept the use of AFR only in exposed places, where many crimes have occurred or which are vulnerable to terror.

The technical possibilities regarding background analysis of video camera data raise discomfort among some of the participants. And some stated a feeling of mistrust the collected data would be used for further analysis which lacks any transparency.

> *If you are looking at the highway entries around Kiel, you will find cameras everywhere. I think they are used to monitor the traffic lights and to detect congestion. If you connect these cameras with the recently introduced automatic number plate recognition (ANPR), you don't even need eCall. Then it will be possible to tell who drove where at what time and some smart programme will be able to determine which exit I used, too.*

2.3 Scanning

Scanning technologies aiming at revealing objects received not very much support among the participants, except for use at airports which is acceptable to the vast majority of participants. Only one person could accept the use of scanning technologies in schools and shopping malls in order to reveal hidden objects, three persons consider its implementation acceptable in public buildings like court buildings and 25 percent would agree to an implementation at central bus stations and train stations. These answers indicate that acceptance is either influenced by already widely implemented use cases. In Germany scanning technologies can hardly be found on a large scale at places other than airports. Especially use in schools and shopping malls is very rare. Another possible conclusion is that acceptance of scanning technologies is higher in exposed places relating to transportation.

The more the specific scanning technology is concerning the personal private sphere of citizens the lower the acceptance rate seems to be. While none of the participants would accept a scanning technology revealing everything beneath clothes, 60 percent would accept a scanning technology where images and objects are projected to a mannequin. In general, scanning technology is acceptable to the participating citizens as only one person found scanning to be never acceptable. Yet, the use of a technology measuring heat, sweat and heart rate was opposed by an overwhelming majority of participants. If a scanning technology is directed at an object (luggage) and not a person, acceptance raises to 70 percent. While a scanning technology aiming at detecting metal objects would be acceptable to 60 percent of the participating citizens.

If scanning technology is applied in order to prevent terror, this purpose does not raise the level of acceptance for scanning technology. The use of scanning technology for detecting hidden objects is – fully or partly – considered an acceptable tool for preventing terror by 60 percent of the interviewed persons. The other 40 percent disagreed completely or to some extent.

2.4 Locating technologies

The general opinion among the citizens concerning locating of cell phones was very similar. Locating technology finds overwhelming acceptance if it is applied to locate suspected criminals or terrorists based on a court order. Only one participant would support a locating of cell phones by police without any judicial oversight prior to the locating. One other participant rejected the locating of cell phones under all circumstances. The broad support for location technologies applies also to emergency situations, in which 90 percent find locating of cell phones acceptable. This measure is considered to be an effective tool for the police in investigating crime. These results clearly indicate that citizens accept locating of cell phones of suspects if an independent power is involved in the decision-making process, or in case of an emergency. Still, 2/3 stated they consider locating of cell phones privacy infringing.

> *If you have your cell phone with you, locating you is always possible. And this locating is related to a person, not a car. I think one should be more concerned about cell phones.*
>
> *But these are only theoretical possibilities of locating, which follow strict rules. The police cannot just locate any cell phone, they need a court order to do it.*

A more diverse picture resulted with regards to locating of vehicles. Just like locating of suspects' cell phones also locating of their vehicles based on a court order received broad acceptance. Again, only one participant could agree to police locating any car – not necessarily only of suspects – without any court order. The interviewed citizens were almost evenly divided with regards to the acceptability of stolen vehicle locating. The use of locating technology to fine speeding and other offences related to traffic found very little support among the participants while automatic accident reporting was considered acceptable by 2/3 of the interviewees. Locating of cars is perceived to be privacy infringing by a vast majority of citizens and a legal provision allowing locating of all cars would be regarded a good tool for the police to investigate and prevent crime by almost 60 percent of the citizens present.

> *I think that eCall is worthwhile. If my car breaks down in the middle of nowhere and no one would find me – if eCall would then activate, I think I would feel a little more secure.*
>
> *Well, if I were the owner of a precious car which got stolen, I would be more than happy if I got it back quickly. But, if all my car movements were stored, this is too high a price to pay and I would rather accept losing my car.*

The mandatory equipment of new cars with the eCall system found support of almost 30 percent of the participants, some of them calling for a possibility to deactivate the system. The majority of interviewees held the view that eCall should be optional, while almost 20 percent opposed any use of eCall.

2.5 Data retention

Data retention was discussed lively in the group interviews. The questionnaire indicates that the majority of participants does not consider the retention of traffic data to be an acceptable tool to prevent terror and even less consider it acceptable for the prevention of crimes. Slightly more than half of the interviewees accept data retention for the purpose of investigation of terror while retention of traffic data for the purpose of investigation of crime finds less support. All citizens oppose the retention of traffic data for commercial purposes. This clearly shows data retention is perceived to be privacy infringing and the vast majority of participants stated this view. The retention of traffic data beyond billing purposes is not acceptable to the vast majority of participants. This deviation from Directive 2002/58/EC is the key result of Directive 2006/24/EC on the retention of traffic data.

> *What really bothers me about these monster- databases is that the data can be used for other purposes, which have nothing to do with the initial purpose. […] Whenever humans are operating systems or if someone can gain personal advantage, you have to expect misuse.*

Combination and alignment of data from different databases receives lower acceptance than retention of traffic data. Even if analysis of data from different databases aims at preventing terror and crime, less than 1/3 of the citizens support such combination of data. Support rises if the analysis is to be conducted *after* a terrorist attack or a crime was committed. In such a case more than 2/3 of the participants find the analysis and combination of data from different databases acceptable. A considerable minority of citizens could never accept combination of data from different sources.

> *What concerned me the most during this meeting was reading about the possibility to collect all kinds of data and then combining it for profiling purposes. That's what stuck in my most and what I find scary.*

Despite of the reserved position towards data retention, more than half of the participants consider it a good tool for police to prevent terror. This shows that even though data retention is regarded to be effective, the level of privacy infringement is considered to be high and data retention is viewed to be an excessive security technology.

Some participants favoured unlimited storage of all data considered necessary by police. Yet, the majority of participants found such a use to be not acceptable.

2.6 Eavesdropping

Eavesdropping is a very common means for German police to investigate crime. Interception of telecommunication has been increased, as an analysis of the Max Planck Institute for Foreign and International Criminal Law described in 2004.

Lawful interception of telecommunications is broadly accepted among the participants, if it is based on a court order and aims at preventing or investigating *crime*. Acceptance for wiretapping based on a court order and aiming at preventing and investigating *terror* received broad acceptance, too, yet not as much acceptance as measures aiming at crime prevention. The obligation for police to obtain a court order prior to wiretapping of communication was essential to the participants for their acceptance of such measures.

With regards to who should be subject of lawful interceptions, half of the interviewees consider wiretapping of suspects acceptable. Some participants could agree to a permission for police to wiretap all communication, without a concrete suspicion. Little support was voiced for an investigative power allowing wiretapping of persons a suspect is expected to contact.

While on one hand the vast majority of participants think eavesdropping is privacy invasive, 60 percent think it is an effective means to combat crime and terror.

2.7 Privacy enhancing technologies

The legal availability of privacy enhancing technologies (PETs) was in general supported by the majority of citizens. Most of them think that encryption should be legally available; a little less support was stated for an availability of anonymous calling cards and identity management systems. Yet, all of the discussed PETs were called for by more than 60 percent of the interviewees. Three participants think that PETs should not be available at all.

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

Chapter 3 Dilemmas of security and privacy

The questionnaire did not only touch questions regarding security technologies as such. The participants were asked about their view on a number of dilemmas illustrating a possible trade off between security measures and privacy impact. Some of the questions raised in this context were also discussed in the group interviews.

3.1 Convenience in travel

The first dilemma dealt with the question whether participants would accept privacy invasive measures which make travelling more convenient. The dilemma was not only presented in relation to air travel where security measures are common and do therefore possibly receive more acceptance than measures at other sites. Instead, also travelling by metro was one presented setting.

The vast majority of citizens could not accept registration of travelling and using fingerprints for payment, even if templates were used. Only if fingerprint data were deleted right after successful payment almost 40 percent would agree to use their fingerprint data for fast and convenient payment in underground travel. However, almost 60 percent of the participating interviewees would under no condition use their fingerprints as identification at the underground. Using fingerprints should not be made compulsory, as a majority of citizens called for having a choice to use different methods of payment.

When asked, whether they could accept thorough registration at an airport database for faster check-in, more than 1/5 of the interviewees would agree to undergo such scrutiny and afterwards using biometrics for check-in. Even use of naked machines at airports would be supported by 1/5 of the participants. Even though it could make check-in faster and thus travelling more convenient, being scanned for sweat, body heat and heart rate found very little acceptance among the participants. Almost 60 percent considered all of the described means for convenient travelling unacceptable and stated they would never give up privacy for convenient check-in at airports.

Even though security measures are common at airports, the majority of participating citizens would not trade their privacy for convenience. While scanning technologies at airports receive some acceptance, support for an extensive background check is lower and as long as citizens remain with a choice, they would rather accept a procedure without thorough registration revealing considerable information about them.

3.2 Preventive anti-terror measures

Even if technologies using optical sensors and a reference database for matching would return no false positives at all, one third of the interviewees would never accept active CCTV surveillance and automatic face recognition. One participant each on the other hand supported either use of AFR regardless of how many false positives occurred or use of AFR with a low rate of false positives. On the other hand, only a little less than half of the citizens insist AFR should only be put to use if it returned no false positives at all. In addition, use of AFR to many citizens is acceptable only in places which are very vulnerable to terror or where many crimes have occurred. Yet, a majority of interviewees would not necessary want to restrict use of AFR only to exposed sites.

As a general result it can be concluded that citizens are concerned of being mistaken for a terrorist. Still, use of AFR, even if returning false positives is acceptable to some and this position is not restricted to use in exposed places.

With regards to data mining and computer aided search aiming at detecting suspicious patterns, concerns about excessive use prevailed. Only two interviewees could agree to an unlimited use of these means and a possibility for police to access all databases available and combining their data. Almost 20 percent rejected all searching and combining of databases.

The vast majority could agree to an approach striking a balance: the police searching and combining anonymous data and in case of a match, lifting anonymity based on a court order.

3.3 Locating technology and possible function creep

The general possibility to locate all cars within a short timeframe is likely to foster claims of using this data for other purposes, possibly related to criminal investigations. In addition, use of location data for business models of insurances is possible, for example for pay-as-you-drive insurances.

Regarding the eCall system, the majority of citizens do support to only use the technology for its currently intended purpose, reporting accidents. In addition, more than 70 percent call for having a choice whether or not to install eCall in their car. Using the location data eCall to provide information for punishing traffic offences is rejected by the overwhelming majority of interviewees. Yet, using the location data to prevent crime or terror is acceptable to almost 40 percent of the interviewed citizens. Only one person would agree to have eCall permanently registering all his movements.

> *We've just experienced what happens in the context of the toll collection debate. First they said, only trucks would be monitored and all other data will be deleted. But then the minister of interior says well, the data still exists and it would be a shame to delete it. And I think it will be the same with eCall. Laws are easily softened. And if a threat exists, all limits are changed.*

3.4 Privacy enhancing technologies

Privacy enhancing technologies are measures aiming at eliminating or reducing personal data by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system.

Even if PETs could be used by criminals, the majority of citizens still value their positive impact for the remaining vast majority of law abiding citizens. Only three interviewees would not accept the use of PETs at all. 2/3 of the participants support availability of anonymous calling cards as well as use of encryption, even if these might make investigations more difficult. Anonymous use of the internet found less support. However, 40 percent support internet anonymity, even if it means persons searching for a bomb cannot be traced. 1/3 of the interviewees would still accept internet anonymity if this means persons searching for child pornography cannot be traced. These positions indicate the high importance of use of PETs for citizens who would only give up this privilege in case of rather concrete indications of a (planned) criminal act.

3.5 Consequences for other people

Finally, the participants were asked about their opinion concerning the consequences for individuals who are not willing to use technologies for privacy reasons or who are not able to use such technologies. An example of the latter would be a person with papillary patterns unreadable by any sensor. A reason for this situation could be hard manual work or diseases like diabetes, where frequent taking of blood samples may lead to scars on the fingertips.

The majority of participants could not accept negative consequences for people who are either unwilling to use a security technology for privacy reasons or who are unable to use a security technology. In this context the interviewees supported the self-determination and conscious decision-making of citizens who are intending to protect their privacy, as only 20 percent of the interviewed participants would accept that people who refuse to use a security technology for privacy reasons are excluded from using some public services. Even less acceptance was stated for excluding people who are unable to use a security technology from some public services: only one participant could agree to such a condition. While excluding privacy conscious citizens from public services found little acceptance, after all almost 40 percent would not mind privacy conscious citizens being excluded from using public transport. Only one participant however could accept if persons unable to use a security technology were excluded from travelling by public transport. These positions indicate that the citizens call upon their government to leave them with a choice of using security technologies and that the government is asked to provide alternative means of using public services for privacy conscious citizens.

Chapter 4 Democratic issues

Finally, the interviewees were asked about their view regarding the decision-making process on development and use of security technologies. Many stakeholders are involved in the public debate on these questions. The citizens were asked to give their opinion about who should be allowed to exert an influence in questions of security technology and privacy. An overwhelming majority of interviewees call for a public debate and public hearings prior to decision-making about implementing new security technologies.

4.1 Democracy and participation

Even though questions relating to security technologies and their possible privacy impact can be very complicated, the citizens nevertheless want to have a say in theses issues. 2/3 of the interviewees hold the view that despite of the complexity of the dilemma of security technologies' impact on privacy, the general public should participate in discussing these issues. In addition, 2/3 of the participants also support including Human Rights Organisations in the debate on security technologies' impact. Lower acceptance was voiced for including manufacturers of security technologies in the debate on important decisions concerning security and privacy. After all, almost 60 percent of the interviewed participants fully or partly agreed to hearing these producers of security technologies before important decisions are made, possibility due to anticipated expert knowledge.

> *Politicians will represent the opinion of the public.*
>
> *I think it is important to include experts. Citizens cannot follow what this is all about.*

The vast majority also called for assessing the level of privacy impact of and alternatives to proposed security technologies.

Furthermore, the majority of interviewees would like to see funding of research projects to be based on a prior thorough analysis of privacy impacts. Yet, almost 30 percent considered an analysis to be of little or no importance at all. With regards to use of biometrics and research thereon, one participant specified his opinion:

> *I think if biometrics is implemented, the state has to make sure that misuse is impossible. And in the end the state has to give research assignments to research companies, asking how to prevent misuse. That is something I expect from the state, that money is allocated to avoid misuse right from the beginning.*

4.2 Proposals

The participants finally were asked about their view regarding different proposals for privacy enhancing use of security technologies.

Regarding the anonymization of data to be searched, almost 80 percent of the interviewees supported making data from unsuspicious individuals anonymous until identification is authorized by a court order.

In addition, it was considered absolute imperative that only authorized personnel can have access to collected personal data. Also, assessing the possible privacy impact of security technologies prior to their implementation is regarded essential by an overwhelming majority of citizens. These positions reflect the mandate to look for least intrusive means regarding citizens' privacy. Also, stakeholders are called upon to ensure that security measures and technologies are not simply introduced to show something is being done to address security concerns. The measure decided for must be necessary and effective (*alternatives*?) and the organisation (private or public entities) using the technology has to implement an access control and a management process ensuring only authorized individuals may access the data.

Chapter 5 Additional information

5.1 Impact of the event on the participants' opinion

All participants were very interested in different aspects of the interview-meeting and the questions discussed, and many of them, as it turned out in the group interviews, had come because of personal encounters with security measures or privacy related incidents. Most participants seemed to have a very clear opinion about their personally desired level of privacy in mind. Thus, almost all participants stated the interview-meeting had not changed their attitude about the issues discussed. Only one participant each explained he felt more positive, respectively more negative about security technologies after the meeting. One participant explained in the interview:

> *Regarding some points – just like probably some other participants, too – I came with a set opinion which I hadn't tested enough. Today I realized that with regards to some points, my opinion isn't entirely convincing.*
>
> *Already having a forum like this indicates that there are institutions having an eye on these questions. The state does function quite well, because we ourselves are an authority of it.*

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

- Annex 3 - Material sent to the participants

- Annex 4 - Questionnaire

- Annex 5 - Transcript of group interviews

- Annex 6 - Frequency tables

- Annex 7 - Comments from the questionnaire