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 5.6 Hungarian report
Interview meeting about security technology and privacy

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

Author(s):
Eszter Bakonyi, Medián Opinion and Market Research Institute

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 report contains the description of empirical evidences from the questionnaires and group interviews conducted in Budapest, Hungary, as a part of the PRISE project. The Hungarian fieldwork of this project took place in Budapest on 11th June late afternoon – early evening. It took approximately 3 hours and integrated 34 persons into a group to think over and discuss together the meaning and the relationship of terms, 'security' and 'privacy'. The situations, characteristics and consequences the participants had to deal with might be also in connection with the dilemma of the role of private and common interests in a society. The meeting and the preparation was organized by the Hungarian Medián Institute which is an independent and experienced research company in the filed of opinion and market research. The Medián involved two experts who assisted a lot in making clear the technological background and the dilemmas of security and privacy for the participants.

Selection of the participants

The Hungarian part of the PRISE project differs a bit from the other five countries' method of recruiting citizens. As it would have been too expensive regarding the modest budget of the project, we didn't recruit citizens by sending out 2.000 letters asking them to take part, instead, we organized it by telephone. We called randomly selected phone numbers (both traditional and mobile phone numbers), informed them about the main parameters of the interview meeting and registered those who expressed an intent to take part in it. Then we had 50 registered citizens to whom we sent out the written materials that were developed by the leaders and partners of PRISE, and afterwards the method was the same like in the other countries. One day before the meeting the organizers called back again the participants by phone to remember the interview meeting the next day. Lastly, there were 34 persons who took part in the group interviews.

The participants' social background

In general, the group's members had a higher socio-economic status than the average in the Hungarian population as they were mostly well educated: nearly half of the group had a diplome, and four tenth had a high school graduation as a highest education level. Only one tenth of the group had lower educational background (in the whole population it takes more than 50 percent). It was a significant and important experience of sample creation and organisation of the interview meeting that – in opposition with the general researches – it was not the participants with the best educational background and the highest social status who didn't show up, but the persons with the lower schooling level. A reason for this can be that the subject can be complicated in itself for average citizens, even for people who studied less, they had to learn about the subject beforehand, to read a rather long text that could be less attractive or tempting for people who are not get used to it. And lastly, another factor could be that the subject itself: notion of human rights and dilemmas on privacy rights can be more interesting or more impressive for people with a higher educational background.

Regarding the other demographic characteristics, the ratio of the two sexes was equal in the group, the majority was in his/ her middle ages, but nearly the same amount of persons belonged to the elderly subgroup, and only one quarter represented the young adults. The majority of the group lived in a family: only one quarter of the group lived in a one-person household. The participants were mostly parents, i.e. two third of them had children, and

usually their children still lived at home (19 out of the 34 had a child, and 13 of the 19 lived together with their children). Most of the group members (29 of the 34 participants) lived in the capital, and only one out of seven lived in the countryside. Regarding their occupational status and professional, the biggest group of the participants worked in the field of finance and economics or business (11 persons: 5 do something financial, and 6 something related to economy), so they may had a special viewpoint on security and privacy, meaning that they might be more conscious about the problem and the dilemma of the two values. There were also some participants who belonged to the educational system (teachers or students, 8 persons). The third group may be characterized by their age: the pensioner and retired people (7 persons). A smaller group was who is in connection with administration (4 persons), and there were some participants whose professional was somehow unique or different from the above mentioned ones (caretaker, housewife, regional health visitor and a translator).

Taking into consideration that the group consisted of people with a rather high social status, it's not surprising that the participants were rather mobile – regarding their travelling habits – and used ICTs. Nine out of ten use mobile phone, and seven out of ten use e-mail and Internet at least once a day. 29 out of the 34 travel by public transport at least daily, and 22 of the 34 participants use a car at least once a week. In contrast, travelling by plane is rather a curiosity for the participants: only 5 out of the 34 travel once a year or more, 18 travel less than one time a year, and 11 participants never travel by plane at all. It may show, and the questions at the discussion in plenum also made the same impression that the participants had more ideas and experiences about ICTs and the security-privacy matters of this field than about the possible technologies and consequences of the problematique of security and privacy, let's say at the airports.

Public attention before the meeting

The research partners of the PRISE project made a short media observation two weeks before the interview meeting. In the Hungarian press there were 46 pieces of news in this period, mostly in the printed press and one report was on TV. Before focusing on the details of this observation we would like to emphasize that selection of this given time period and the mediums cannot show credibly the Hungarian public's feelings and debates, but anyway, it was not our aim. The media observation of a longer time-period and the inclusion of a high-scale or mostly all media (printed press, TV, radio, Internet) would have gone beyond the possibilities of this research. On the one hand, we didn't want to focus on the significance or importance of the given news, so we didn't compare the frequency of a concrete issue with other events and news. On the other, we also didn't want to test if the participants knew about these pieces of information, so we didn't want to know if the news had an effect or not on the participants' views. The reason why we made this media observation was rather to represent the main topics and the main emphases touched by the media just before the interview meeting in the filed of security.

The majority of the news and articles (13 of the 46) was about security in IT and on the Internet, 7-7 dealt with visa matters (the possible e-visa for EU citizens travelling to the US that will store their personal data) and RFID, identification of objects in border control. 6 articles wrote about the Galileo program, 4 informed about the misuse of personal data by banks (accidentally, and about data retention). 3 wrote about locating technologies and 2 about the more convenient travelling by security technologies. There were 4 other topics that we couldn't group, one about CCTV cameras, one about eavesdropping, one about lie-detector, DNA and about security-privacy dilemmas, and one about scanning technology. In addition, there was a serious police scandal that interested the Hungarian public in that time. A young

girl suspected five policemen of raping her in the street. Although, the policemen and their representatives denied all the time and the case is still not finished, the public could get some information about security technology when the media showed that the standpoint of the policemen could be disproved regarding the records of CCTV cameras and the location of their car's movements by GPS in that given evening and night.

Participants' interests at the meeting

The participants posed a lot of questions to the expert and in general, they were very open and active after his lecture. The questions mostly dealt with the privacy problems or some negative consequences that security technologies may generate. There was a question about a Hungarian community website called wiw (Who Is Who?) or iwiw which is a kind of register or database for constructing personal networks by making the own and also the friends' personal data public and visible on the Internet. The participant was wondering if it was data retention and whether it had serious privacy infringing consequences, so is it dangerous to take part or not. The second question was whether the expert could tell an example about the situation when the restriction of human rights may help the interests of the terrorists. Another person said he asked politicians via e-mail and tried to search on the Internet to know what things could happen without that citizens' knew about it, but he didn't get answer and asked how politicians got information about these issues. The fourth one wanted to know if the contracts (when for example, buying a mobile phone) contain the technology's effects on privacy. The next one was wondering if a secret police or a police with stronger rights for recon would solve the problem of security of the society. The fifth question was that for how long the mobile phones have been located and recorded. And the last one was that if the participant is called by a company s/he doesn't know, does s/he have the right to know how they got his/ her number and if the conversation is recorded or not.

The participants were very active and constructive during the whole meeting, they took it seriously that their opinion count and they are discussing and asked about a significant social issue. They found this whole activity very 'scientific' in a positive way, especially, when they referred to the expert's presentation, and they liked the whole method of the research, the participatory approach. Although, they were very satisfied, cooperative and optimistic about the idea of the research and the way it was conducted, they were much more sceptical and pessimistic about the handling of the results, namely, they supposed that it would be taken into a shelf and politicians wouldn't take into consideration what citizens prefer or worry about.

Purpose of this report

The analysis tries to focus on the general attitudes of the citizens towards different security technologies – also in general and separately the given equipments –, the question of their using methods, namely, who and in which situations should use them to achieve security for society, and what kind of privacy dilemmas are induced while developing and introducing these technologies. The main aim of this research was not to show the Hungarian public opinion that what security technologies should be used and in which places, or what security technologies shouldn't be used because of privacy reasons. Not only because we wanted to focus on something else, but also because of the small number of the participants. The aim of the research was in real, to highlight the latent cognitive schemas and the argument structure of citizens when it comes to new security technologies and safety of individual privacy. In this brochure the main points of the research will be presented in different chapters, and keeping in mind the focus of the research there is no too much statistical tables, no statistical tests or multi-variable models, we rather used the numbers to show some tendencies in the data. But of

course, all frequency tables of the questionnaire data can be found in the Appendix. We put only those tables in the text when it was a generated variable that was not in the questionnaire per se.

Executive Summary

The participants expressed a partly ambiguous and partly sceptical view on the effects or usefulness of security technologies. As they summarized it, the causes of terrorism should be abolished to solve the problem of insecurity, thus, it's rather a social than a technical problem. The tools they suggested to use for this reason are education, integration and making better economic conditions.

Participants mostly talked about eavesdropping, locating technologies and data retention at the group discussion as technologies that caused significant anxiety for them in relation to privacy, and they expressed more acceptance towards biometrics (in airports, usually) and CCTV cameras that they have already known better before the meeting.

The group recognized a lot of advantages of security technologies, even in other fields of life, although, they also kept in mind that these technologies can be privacy infringing. They mentioned that these technologies might generate social trust, or make life easier and more convenient, and that social relations could be easier to make and sustain. They also mentioned the preventive effect of security technologies and that these could decrease the number of criminal actions, although, they also added that these technologies were rather efficient against the less serious criminals (thefts for example).

They preferred security more than privacy when the situation relates to public places and crowded social events; privacy usually got a priority when the dilemma related to the private sphere. Another situation when security or convenience can be more important than privacy if it's optional, so the person can decide to use a technology or not. But when it was not a question of personal decision of using a security technology or not, but something that has to be applied by all members of the society, some tended to be more 'civil rights activist'.

They preferred very much to ask the citizens – which technologies and how should be used – when politicians were mentioned in the question. In contrast, when citizens' role in discussion and decision-making about these matters was not in relation to politicians, but to security and/ or privacy experts, the participants preferred to give a more slightly importance to the general public and everyday people. The human rights organisations also got high priority in being involved into the debates as it's also out of the sphere of politics and closer to the citizens and the civil society. Opinions about the role of private companies that produce security technologies were much more complex and nuanced: the group was much more divided whether these companies should be asked.

The evidences show that people are worried about monitoring all persons by the authorities, but they are much more worried about misuse of collected data by the organisations and authorities.

Chapter 1 Participants' general attitudes

According to national and comparative international researches, scepticism, pessimism and a 'negative way of thinking' are a significant part of Hungarian identity – both from outside, defined by others, and from inside as self-definition (see for example: Eurobarometer: European social reality, 2007). (Another important element is 'creativity' that was also mentioned among the advantages of developing new security technologies, see chapter 2.1.8.) This disposition could be observed when the participants were asked about their general attitudes about security and privacy, and also at the reasoning behind the opinions they expressed at the interview meeting.

> *The problem is that more and more negative things are made public (police scandals, etc – E.B.), so one starts to concentrate rather on the possible negative effects of a new thing being introduced. What may go wrong out of it? We should change somehow our worldview. Hungarian people are typically like this.*

This general disposition can be found both in the interviews and the questionnaire answers – as they expressed a partly ambiguous and partly sceptical view on the effects or usefulness of security technologies. There was a common understanding or consensus that creating and preserving a secure community or society is not or not just a matter of technology, it's rather a subject of social issues. As they summarized it, the causes of terrorism should be abolished to solve the problem of insecurity, thus, it's rather a social than a technical problem. The tools they suggested to use for this reason are education, integration and making better economic conditions.

> *The causes that generate terrorism should be abolished.*

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

Similarly, regarding the quantitative data, the most polarizing question was among the general issues: if the security of society is absolutely dependent on the development and use of new security technologies or not. 14 of the 34 participants didn't agree with the statement, and the remaining part of them divided into two almost equal groups: 9 who agreed on dependency on new security technologies, and 11 persons couldn't decide. Although, it doesn't mean that the Hungarian group was against these technologies or was suspicious with these technologies as 20 out of the 34 participants agreed on using security technologies if available, and only 2 persons disagreed. It can be also mentioned that it was the question where the most (12) uncertain answers were made.

Trust in security technologies may be also in connection with a general positive or negative attitude towards technical equipments and with being get used to these new things. If we take the differences between the opinions according to the social background of the participants, we can see that mostly the men and the younger persons are in favour of the new security technologies and agreed on the above mentioned two statements more than the others. The educational background didn't make an important difference in the attitudes towards general

advantages of using new technologies. Opinions about security technologies may vary so much between the persons with or without a child as the formers may have a special view on the importance of security in everyday life. If we keep it in mind, we can see that the participants with a child really took more seriously that if we have security technologies, we shall use them, but they don't agree much more with the statement that the society's security is very much dependent on these technologies. The real difference between the participants with and without a child was that those who have a child had much more sharp or polarized opinions about it (so, people who have no child answered 'neither agree nor disagree' by a higher rate). The relationship is similar whether there's a child living at home or not.

Another general attitude was that things go in a bit different way in Hungary than in Europe, regarding the democratic principles or procedures in practice, or the functioning of institutions. They referred to the violence took place in autumn in Budapest, and the scandals of the police turned out in the last months (abuse and corruption). So, this attitude can be inspired by these latest internal political events and not a general worldview.

> *These systems, here in Hungary, don't work the way as they should work.*
>
> *I have the same problem as you that basically, things don't function in Hungary. I don't know why but nothing works as should work. Anything that is tried to introduce turns into the opposite. And then it's over, or it's forced a bit and gets better, but not really works.*
>
> *My personal opinion is that at the certain autumn events (siege of the Hungarian national TV – E.B.), 'accidentally' nobody (of the policemen) had identification sign which is said to be illegal. If it was illegal, it may inspire a way of thinking that maybe laws don't prevail for us as for the others, and we may do things that others cannot.*

Although, there is a general scepticism towards bureaucracy in general that emphasized the disfunction of organisations: 19 of the 34 persons agreed on the statement that many security technologies do not really increase security, but rather applied only to show that something is done against terrorism, and just 6 disagreed (9 were uncertain about it). The participants' social-demographic background doesn't make a difference in the opinions, except the peculiarity of being a parent or not. The participants who had a child were more sceptical than the others towards institutions and leaders in deciding about, implementing and applying security technologies.

But trust in Hungarian institutions is not destroyed completely by the events of the near past, when it comes to the abuse or misuse of security technologies, participants expressed more doubt towards criminals than governmental administration. However, the majority (22 out of the 34) agreed upon that governmental agencies are likely to abuse security technologies and 7 persons disagreed, but much more participants: almost everybody thought the same about criminals (31 agreed on possible abuse by criminals). There were some differences in the attitudes of different social groups. Men were worried more about misuse of security technologies by criminals, while women about the misuse by governmental authorities. Also the younger participants and those who have a child were a bit more anxious about the misuse by criminals, and the difference was even bigger between parents and non-parents about the danger of misuse by governmental authorities. Although, it's a bit contradictory with the above mentioned that those participants who don't live together with a child are more worried about

the security technologies' abuse by criminals, but we have to add that the number of participants is too less to draw comprehensive conclusions.

When we mentioned 'criminals' in the questionnaire or during the interviews, they showed a higher awareness about the subject and the possible dangers, but when we mentioned 'terrorists' they were not really worried about it and didn't really think seriously about it, as they thought terrorism was not a real and realistic problem for Hungary. There was a general attitude that it cannot happen to us, terrorism is rather far from this region.

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

Regarding the problem of privacy infringement, the Hungarian group was rather worried about it. The majority (19 of the 34 participants) disagreed on the statement that 'if you have nothing to hide, you don't have to worry about security technologies that infringe your privacy', and only 8 agreed (7 were unsure) – especially those who have no children. Also the majority (25 persons) emphasized that it's uncomfortable to be under surveillance – even if you don't have criminal intents –, and only 6 didn't care of it (3 were ambivalent). There was also nearly unanimity that privacy should not be violated without reasonable suspicion of criminal intent: 26 agreed on it and only 6 of the 34 citizens disagreed (2 were ambivalent). The reason of this general refusal of endangering privacy may be on the one hand that privacy is an important value itself and the statements were rather simple, not contrasted with other basic values. On the other hand, privacy might gain a higher importance after the end of the state socialist regime when people's right for privacy was infringed considerably.

> *Briefly, the general human defencelessness. Big Brother. … Information means power.*

Regarding the differences between the participants with a different social background, the younger, well-educated people felt more uncomfortable to be under surveillance than the others. And in general, those who have children or whose children live at home were a bit more sensitive to the importance of privacy.

Chapter 2 Security technologies

After the general issues, the participants were asked to express their attitudes towards the concrete security technologies and the way how they would prefer to use them by the authorities. Regarding the technologies that were mentioned in the questionnaire, participants mostly talked about eavesdropping, locating technologies and data retention at the group discussion as technologies that caused significant anxiety for them in relation to privacy, and they expressed more acceptance towards biometrics (in airports, usually) and CCTV cameras that they have already known better before the meeting.

2.1 Biometrics

The group had mostly positive feelings towards biometrics when it was about using fingerprints. However, one third of the participants (10 of 34 persons) were totally against of using biometrics for access control. One reason was that some associated the use of fingerprints with investigation of crime.

> *The starting point is offensive. That conventionally, fingerprints are usually taken from criminals.*

The majority (20 persons) of the remaining part of participants would feel comfortable using fingerprints, but facial characteristics and iris recognition were chosen by just a few people (8 and 6). Although, only one third of the participants would feel uncomfortable if they should use biometrics for access control, 30 of the 34 persons could say at least one place or situation when using biometrics may be reasonable. They prefer biometrics mostly at the airports and border control (29 and 22 persons), but also a lot of them (16 of the 34) would accept it in banks. A minority think that using biometrics would be reasonable at central bus and train stations (8 persons), in stadiums and other crowded events (8 persons), but they refused the usage in stores and other private services (1 and 2 participants would accept). It would have been interesting to compare the acceptance of using biometrics at the airport according to the frequency of travelling by plane, but in the Hungarian sample there were only 5 persons out of the 34 who do it one-two times a year or more, so we cannot compare it. The same problem occurred at comparing the acceptance of biometrics for entering central bus and railway stations according to the frequency of using these places, as again, only 5 out of the 34 participants travelled by public transportation on less than a daily basis.

The group was very much divided on the consequences of using biometrics. The opinions were very polarized whether a central database containing the biometric data of all citizens would be an acceptable step to fight crime. One third agreed on the statement that it's acceptable, one third disagreed on it, and another one third of the participants were ambivalent about the subject. There were also differences between the views on insecurity of biometric passport. Half of the participants expressed anxiety because of the risk of biometric data being stolen. One quarter of them did not feel insecurity about using biometric passport, and another quarter of the participants had diffuse feelings about it. But at the group interviews they admitted that the present passports also reduced persons to numbers and identification data, so the feeling doesn't change much.

> *Technology cannot be stopped, the world is developing and we also have to, we cannot choose. … Just think about the passport, we were also rebelling against it that it identified us by numbers as if we were cows, everybody was arguing, but couldn't do anything about it and we got our numbers. And one could know everything about us,*

all data. (passports contained more personal data before the regime change in 1989 than now – E.B.)

Another opinion expressed at the meeting was that biometric passport makes life more convenient as reduces bureaucracy.

This biometric passport would replace identification cards. I shouldn't bring a lot of papers with me, I should have and show only my passport. … I would need only one, and not five. So I wouldn't need identity card, driving license. I shouldn't extend the validity or renew it as my fingerprints won't change. So, it would save me, if I see from this point, from a lot of things, I shouldn't go to the office of personal documents, I wouldn't be afraid that somebody will steal it from me.

2.2 Camera surveillance

The answers were more homogenous about camera surveillance, maybe because it's more well-known in public places as biometrics are a rather new technology than camera surveillance, and as it's been already used in some places, so the participants can be more used to it.

Moreover, the gains of using cameras seem to be recognized by the citizens as two of three participants would urge to use more. Six of the 34 were satisfied with the number of CCTV cameras in public places, and only two persons wanted less and 2 rejected this technology at all. These cameras were very much accepted in airports and banks (30 and 28), and still half of the participants (18 persons) would accept it in stadiums and other crowded places or events. One third of the group prefer CCTV cameras in stores, and another one third wouldn't make a difference but accept it in all public places. Nearly nobody (4 of the 34 people) would prefer cameras in dressing rooms, and only one couldn't name a place where this technology could be accepted.

The Hungarian group's attitude was rather supportive towards camera surveillance. The majority (two persons out of three) expressed that they feel more secure of this system, and only 3 disagreed on it. Although, some people, 9 persons were ambivalent about it, and the group was more divided when it came to the question of privacy. Approximately one third of the group had the feeling that cameras infringed their privacy, and one third disagreed with this statement. Another one third couldn't choose between agreeing or disagreeing whether CCTV surveillance endanger their privacy or not.

Although, some critiques were also drew up at the group discussions. Some participants had bad experiences with CCTV cameras as they are always under surveillance when they work.

Cashiers are eavesdropped and watched by cameras, much more than the customers who even steal. … We told a customer not to buy a product as the expiration date passed or we couldn't help them how much was a product as we don't know the codes. … It was not our fault, but then we were questioned and some were fired. What's the sense of it?

I work in an exchange counter, and once a man came back – I'm watched by a camera, moreover, by two cameras – and accused me that I gave him 10.000 Romanian Leus instead of 10.000 Hungarian Forints. And from this point of view, it was good for me. But I hate it, I don't like to replay and look back myself, as I eat and everything like this.

In sum, half of the participants had a strong standpoint about the dilemma of security and privacy in relation to camera surveillance, and half of them (17 persons) had somehow ambivalent feelings about it. The majority of the people who had a strong viewpoint about this dilemma (10 persons), said that the cameras make them feel safe and they have no privacy problem with them. The remaining part of the group (7 persons) was anxious about the privacy consequences of camera surveillance: 4 participants agreed that cameras make them feel secure, but at the same time uncomfortable because of privacy infringement, and 3 participants expressed consequently that they didn't feel secure by the cameras and rejected this technology because of the importance of their privacy.

Generated variable on security-privacy dilemma of CCTV cameras

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00 safe+accept	10	29,4	29,4	29,4
	2,00 safe+reject	4	11,8	11,8	41,2
	4,00 not safe+reject	3	8,8	8,8	50,0
	6,00 ambivalent	17	50,0	50,0	100,0
	Total	34	100,0	100,0	

At the interview meeting there was a debate on whether the location of CCTV cameras should be public and known by anyone or the authorities should keep it in secret. Some argued, it has no real effect if the criminals (or the drivers overrun the speeding limit) know that they are watched, but others thought it could also have an effect if the cameras are visible, and on the other hand they wanted to have the right to be informed about surveillance.

> *What is the reason for this if everybody knows that the camera is there? In my opinion, it's somehow nonsense. People shouldn't know where it is, neither the speed checking module, nor the camera, because this is the case when it's effective. … If I know that there is speeding control at the 67th km and the 83rd km, then I'll drive fast and slow down there.*
>
> *Yes, it should be defined at which places it should be known if there is a camera. At a speeding control nobody will mind it, but in other places one may. …*
>
> *After all, if there is a note saying that a camera is being set up somewhere, it can result that somebody having bad intentions goes there and says: 'I would find another place where there's no camera. And then it's prevention. …*
>
> *Nothing should be hidden of us. Rather, we should be informed that this and that is applied here.*
>
> *… it could be abused. So, they could send letters about penalty saying that 'we saw you or shot you somewhere and you have to pay something', but you didn't see them.*

Although, some emphasized the preventing role of CCTV cameras, others were sceptical about the whole idea.

I cannot find too much sense in a system like this. I will know if Ali or Mahmud exploded the metro coach. How does it help us if 50-100 people have already died? We don't know before it that he is a terrorist.

2.3 Scanning

Participants were rather flexible with the scanning technology and its application: they accepted mostly all cases and methods listed in the questionnaire, except total scanning that shows everything under the clothes, and scanning in shopping malls. As a participant explained it:

It was the most terrifying for me when it was written that it's necessary to go through these kinds of gates when entering a shopping mall. It's really too much, because it's okay that one is shopping, but let's say, if one goes there just for having fun. And then if I imagine that I thought I would have had a pleasant day, shopping and whatever, I go to a cafeteria, and then I have to go through a cell and security guards, that's too much.

But they find scanning necessary at the airports (all 34 participants), public buildings e.g. courts (22), and some in schools (13), central bus and train stations (13). Only a slight minority (7 participants) thought it to be necessary in shopping malls. Regarding the concrete scanning methods, the most accepted ones were when hidden objects are projected onto a mannequin (27 persons) and luggage scanning by x-ray (27 persons). Also a majority (22 of the 34) would accept the scanning of metal objects, but revealing everything under the clothes or scanning body heat, sweat and heart rate were rather rejected (only 4 and 9 accepted).

The reason why the participants had rather accepting disposition toward this technology may be that this method could prove rather well the concrete, practical effectiveness in strengthening security. The majority of participants (25 of the 34) agreed that scanning of persons for detection of hidden items is an acceptable tool for preventing terror. It may give a stronger acceptance for this technology – although, they recognized also the disadvantage as it may harm privacy or can be uncomfortable, – as they criticised CCTV cameras for being useful rather 'after' a crime or terror attack to find the bad guys, not 'before' to prevent it, but about scanning it's more accepted to be an effective tool to prevent these cases. Thus, only 5 of the 34 find it unacceptable and 4 were confused about the subject.

2.4 Localization technologies

People preferred using localization technologies if it was not in general, but for special reasons. For example, the strong majority supported the locating of mobile phones of suspected terrorists and criminals (32 of the 34), and the locating of suspected criminals' and terrorists' cars (28) – if in both cases, based on a court order. But without court order, the majority (30 and 28) rejected this possibility. The participants chose security to be more important than privacy if something bad happens. 30 out of 34 would allow locating of mobile phones in case of emergency (accident, lost children, disoriented persons), 29 found acceptable locating cars after accidents (and to start an emergency call), and 28 to find stolen vehicles. Not surprisingly, they mostly wouldn't use this technology to control speeding and penalize the speedsters (9 of the 34 accept it). Only one person said that he could accept locating neither mobile phones, nor cars.

Those who travelled less often by car would imagine more situations when locating cars is acceptable, although, these differences are modest. A bit more people of those who use car less often than once a day would accept a bit more to use location technologies by the police to find stolen vehicles or in case of an accident to locate the injured and call for help. And these people were much more in favour than the others of using this technology by the police authorities without a court order. These empirical evidences – however, based on a very small sample – show that people are more cautious or distant with a security technology if it has a more significant impact on them (and their privacy). It would be also fruitful to compare the attitudes towards locating mobile phones according to the frequency of mobile phone usage, but unfortunately, nearly the whole group (31 out of the 34) use mobile phone on a daily basis, so we cannot really compare it.

If we take the 'special' cases of locating technologies, when these are used for police investigation to find criminals and terrorists the group was very much in favour of this technology. 28-28 participants agreed that locating mobile phones and cars is a good tool for the police in investigating or preventing criminal and terror attacks. But when the question is general they admitted their worry about the consequences on personal privacy: 17 and 18 people thought locating all mobile phones to be privacy infringing.

The difference in this subject between participants who use cars often or rarely was that those who use a car more often agreed more that it was privacy infringing, and those who use a car less than once a day were more uncertain about the privacy consequences of this technology. And again, we cannot compare the attitudes towards locating technology of mobile phones and privacy infringement on the basis of the frequency of mobile phone usage.

In the group discussion they also emphasized the privacy problems in relation to locating technologies, the feeling of defencelessness, but they mentioned some practical advantages, too, e.g. in case of an accident or emergency. Or when the locating of mobile phones may have the opposite effect: it doesn't only show an authority or service where the given person is, but also for him/ her having the mobile.

> *In the underground I can see on my mobile phone at which station we are right then. Of course I know, but it's better that the telephone also shows it. If I were in an unfamiliar place, it would be important information.*

The group was very much divided whether the eCall technology should be automatically installed into new cars or not. One third of participants preferred it without any restriction, one third would accept it if it's possible to deactivate, and another one third found it important to have the choice not to install it if a customer doesn't want it. The answers were very diffuse according to the usage of cars. Those who drives on a daily basis chose more often the two extremes (to install eCall automatically into new cars, and never install it at all), while those who travel by car less often rather chose the more permissive options (to install the technology but with the possibility to deactivate it, and to make it optional for the purchasers to decide whether they want to have eCall installed or not).

2.5 Data retention

As we have already mentioned at camera surveillance, the participants were a bit sceptical again about the possibility of preventing terrorist attacks when it comes to communication data retention or scanning and combining different personal data. The majority (21-22 persons) found it acceptable to store communication data or combining different personal data in a huge

database for investigating criminal and terrorist actions which already happened. But when the question was the same just it was about the preventing role of these technologies or methods against terrorism, much less people accepted them: 17 supported communication data retention and 14 the scanning and combining of personal data from different databases. Although, they were not that sceptical about preventing criminal actions by storing communication data: 20 found it acceptable, but they again, supported modestly (only 14 participants) combining personal data for preventing crimes. One sixth-one sixth of the participants rejected these methods, i.e. 4 rejected both of them, and another 2 persons rejected data retention of communication traffic, another 2 persons were against combining different personal data into one database. The group was very negative with using these technologies for commercial purpose.

However, people found data retention acceptable for investigating crimes and terror attacks, as there is a significant hesitation and scepticism towards the functioning of democratic institutions in Hungary (since last autumn), the group was very much divided whether government institutions and authorities should have a strong role in this issue, namely to decide which data and for how long should be stored by them. One third of the group (13 of the 34 participants) wouldn't delegate this decision to government institutions and authorities, another one third (10 persons) would accept it. The remaining one third couldn't decide exactly if it's good to let the central authorities to store all data they find necessary for security reasons, and as long as they find it necessary. Regarding the usage of ICTs (e-mail and Internet), those who use more, disagreed more with this statement, however, there was no difference in the rate of agreeing with it. Although, the participants agreed on the usefulness of data retention of communication traffic for investigation purpose, nearly the two thirds of them (19 of the 34) wouldn't support storing of the data of telephone, mobile phone and Internet communication beyond the necessity of billing purpose. One third was ambivalent about the subject, and only 4 persons disagreed with the majority of the group. And there was no real difference about this issue between those who use ICTs on a daily basis and those who don't.

The group was also very much divided whether combining and storing data from different personal databases is a good tool to prevent terrorist attacks. Again, one third (12 participants) agreed on this statement, another one third (10) didn't accept it, and the remaining one third (12) had ambiguous feelings about it.

The Hungarian group had a rather complex view on this subject, as they couldn't really deal with the dilemma of privacy and security in relation to data retention. On the one hand, there is a strong support towards this technology when it comes to improving police investigation of crime and terrorist actions. But on the other hand, there is a significant worry among the participants regarding the privacy consequences. The majority of the group (21 participants) expressed that scanning of and combining data from different databases containing personal information is privacy infringing, and only a few people (4) held the opposite viewpoint. Those who don't use ICTs at least once a day were worried much more about privacy infringement than those who use these technologies more often – and maybe it's one reason why they use it more often. Some (9 persons) couldn't decide between agreeing and disagreeing. Moreover, the group was very strongly against the phenomenon of function creep. Nearly the whole group strongly agreed – 31 of the 34 completely, 3 partly agreed – that databases being used for something else than the original purpose was a serious privacy problem. And again, those who use e-mail and Internet less often were more anxious about function creep. The participants spoke about their worry at the group discussion too that it's a real problem that personal data can be fallen into 'bad', evil or unauthorized hands.

These technology equipments are essentially good. There is a very big problem with them, a huge distrust that if I apply it, I don't know what they'll use it for.

Our data are combined in a specific system. But those can also be broken down.

At the refund of medical visiting fee, it showed that some people can get data that they don't have anything to do with. For example, they will know with which illness you were in hospital. It's about the municipality's notary. … He has nothing to do with it. … Let's say, you have AIDS and that's why you have to go to doctors. And then you have to go to the notary and say, 'oh yes, I go there because of this'. How is it?

2.6 Eavesdropping

Eavesdropping was an easily understandable technology also in itself, and as a security-privacy problem. Maybe because it's more well-known than, for example, the different scanning methods and locating technologies or data retention. It can be a reason why this technology was very much supported by the participants – 29-29 of the 34 members found it acceptable in case of investigating and preventing crimes or terrorist actions –, but only if this method is always authorized by court order. Without court order only 7-7 persons could support it, and nobody would allow it for commercial purpose. Only 2 participants rejected eavesdropping at all.

The majority of the group (two persons out of three) think that the police should use this technology only against suspected persons, but the remaining one third (10 persons) would allow the authorities to use eavesdropping in case of persons expected to contact the criminal or contacted by the criminal.

The participants, again, couldn't really deal with the dilemma of security and privacy in case of eavesdropping, i.e. they preferred using this technology by the police forces, but in the same time they kept in mind that it's very much violating to personal privacy.

What would really disturb me is, for example here with the mobile phone that I don't know how long it's stored whom I talked with. Or for which reason it is used that I talked to somebody or what I was talking about.

Two participants out of three agreed on the statement that eavesdropping is a good tool for police investigation, and the same ratio of them agreed that this method is a serious violation for privacy. 10 and 9 persons were ambivalent in these subjects, and only 3 and 4 disagreed. In sum, half of the group was somehow unsure or ambivalent about the dilemma of security and privacy. The majority of the people who held a certain position (10 out of the 17) agreed that eavesdropping is a good tool but violates privacy so much. Only 4 persons thought that it was a good tool and didn't infringe personal privacy or not that much, and 3 were very sceptical expressing that eavesdropping is not really a good tool for investigation, but violates so much people's privacy rights.

Generated variable on security-privacy dilemma of eavesdropping

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00 good+not violating	4	11,8	11,8	11,8
	2,00 good+violating	10	29,4	29,4	41,2
	3,00 no good+violating	3	8,8	8,8	50,0
	6,00 ambivalent	17	50,0	50,0	100,0
	Total	34	100,0	100,0	

The empirical evidences also showed that those who use ICTs more often are less worried about the privacy violating consequences of eavesdropping.

2.7 Privacy enhancing technologies

Privacy enhancing technologies (PETs) in general were strongly accepted by the group, and they wouldn't restrict this right of people to hide and remain anonymous if they want even when it comes to hindering of police investigation. Regarding the numbers, 29 out of the 34 participants agreed that these technologies are necessary in today's society to preserve privacy (only 1 disagreed), and only 11 persons agreed that PETs should not be legal if they make police investigation and prevention of terror and crime more difficult (13 disagreed and 10 was ambivalent about the subject). Those who use e-mail at least once a day agreed a bit more than the others, and those who use Internet rarely agreed more that PETs are a necessity in today's life to preserve privacy of the citizens.

Although, the participants emphasized the role and importance of privacy enhancing, when they had to choose between the concrete technologies, their preferences were rather diffuse. Half of the group (17 persons) preferred encryption programmes, and 15-14 participants said identity management and anonymous calling cards to be important to have legally by everybody. 5 participants rejected availability of PETs for everybody, and 4 persons couldn't answer the question. That is, 'only' 25 of the 34 people would prefer at least one of the PETs listed in the questionnaire.

It can be interesting that those who use e-mail and Internet the more often preferred less to make PETs legally available for all citizens. On the other hand, the reason for this may be that those people who use these ICTs more often simply don't worry that much about the infringement of their privacy – and also it may be the reason why they use it rather often. In case of anonymous calling cards we couldn't compare whether the frequency of usage make a difference in the opinions as nearly every participants used mobile phone on a daily basis.

Similarly to the above mentioned, some participants at the group interviews expressed that there were too much emphasis on privacy rights in the scenarios, and they didn't think security technologies to be so dangers in this way.

> *We have to restrict our freedom in some degrees to have security.*
>
> *It emphasized the human rights for freedom too much.*

This threat written here is inadequate.

2.8 General attitudes

At the group interviews some participants expressed that they were aware of the privacy infringement character of most security technologies, but they also added that it was impossible to live in fear, so it would be better not to think about it all the time. Also some participants highlighted the importance of the perception when it comes to security and privacy, and they said it was better to be monitored indirectly when they either didn't know it, or rather they knew about it but the technologies were hidden or not that noticeable. They said they would have felt these situations more comfortable if they had known about the CCTV cameras but couldn't have seen them at every corner.

In general, the group recognized a lot of advantages of security technologies, even in other fields of life, although, they also kept in mind that these technologies can be privacy infringing. For example, they mentioned that these technologies might generate social trust, or make life easier and more convenient, and that social relations could be easier to make and sustain. They also mentioned the preventive effect of security technologies and that these could decrease the number of criminal actions, although, they also added that these technologies were rather efficient against the less serious criminals (thefts for example).

More criminals can be caught. The petty criminals. Which may be the majority.

Another advantage was that they mentioned, although, it was not discussed very deeply or detailed, that these new security technologies can improve the development of the Hungarian industry and the Hungarian intellectual capital as it will be a necessary innovation in the EU, so investment will come into the country.

A new industry! It's one advantage of it. And also, the intellectual capital in Hungary is rather strong. We would be good at this.

Among the disadvantages, they referred to, naturally, the privacy infringing characteristic of most security technologies, and the 'dehumanizing' mechanism while using these equipments or when a problem occurs.

If something goes wrong, there's no alternative, there's no a person who would say that the system is out of order, and instead, would ask for a personal data, let's say the mother's name. It's impossible to substitute it, there is only one way adopted, and if something doesn't work…!

They also mentioned that some journalists had hidden some prohibited objects and could have gone through the security controls that had made them distrustful towards these technologies. Maybe they were anxious the most about security technologies when data collected about them is used for a different purpose than the original one, or that they cannot know who can have access to these technologies and data. Maybe, it was the disadvantage that was mentioned in all groups during the group discussion. But, there was also a constructive suggestion about being monitored all the time:

Actually, it's insecurity that one can feel, because there are a lot of 'black holes' around us about this subject, … those who use the Internet are totally 'denuded', everybody is so defenceless as if they put their latchkey under the doormat. I don't

know, it disturbs me terribly. I would like a few things, if I travelled, I wouldn't go to Syria or Egypt, but if I went there and a 'follower' or an emergency call equipment would be set up on me and I ask to activate it and to monitor if I'm still okay, I would like it. But I don't like that people whom I don't know and who don't introduce themselves search for me and find me from 'mysterious' places that I don't know.

And moreover, some of them were sceptical if the security of society is a matter of technologies. They emphasized the approach or worldview of the people – both of those who make the control and who are controlled –as an important factor to achieve security and saying that the problem is the low level of social morality.

These are not the security equipments, facilities that would improve our security, but rather an approach.

It's about people's morality, … There shouldn't be fast drivers just because a special equipment or technology doesn't let the car go faster, but because the person decides like that.

It's shocking when the security staff does it in an offensive way. It should be done that I feel that s/he does it for my interest. … It's humiliating to be taken away when all the other travellers watch at you when a problem occurs at your control. They don't handle these situations with the discretion they should.

Chapter 3 Dilemmas of security and privacy

After thinking about the main phenomena and consequences of security technologies, participants were asked to hold a more concrete (or less ambiguous) position, namely, to choose between the value of security and the value of privacy in certain, already defined situations. In generally speaking, they preferred security more than privacy when the situation relates to public places and crowded social events.

> *Security is more important than privacy: when travelling by plane. So at those places when people are in a closed location and there's no way out of there. Because, any way out of there will end in a tragedy.*
>
> *In case of bank robberies.*
>
> *In sport stadiums.*
>
> *Cinemas.*
>
> *Crowded places.*
>
> *In public places I accept that it serves the community's benefit. In clinics and places like this. In hospitals, crimes also happen there.*

And privacy usually got a priority when the dilemma related to the private sphere.

> *Private sphere is more important than security: at home. … One can coordinate him-/herself about what issues s/he wants to talk about. S/he knows whether s/he can talk about that or not. … But it shouldn't be seen by everybody if whatever, what I'm doing in the toilet.*

Another reason for situations when security or convenience can be more important than privacy if it's optional, so the person can decide to use a technology or not (See the example in chapter 2.8. about travelling in some 'problematic' Arabic countries). But when it was not a question of personal decision of using a security technology or not, but something that has to be applied by all members of the society, some tended to be more 'civil rights activist'.

> *I would say that if we now talk about security technology, I realize that if it's about my car if an accident happens to me, so the emphasis is on 'me', so the viewpoint is 'me', then I accept security technology in itself and its application. But when it comes to groups, and it has to be used in a greater, broader public, then I may say that 'oops!', it disturbs me already and it's a burden for me.*

3.1 Convenience when travelling

The first case when they had to decide what is more important for them was the question of convenient and easier travelling vs. preserving privacy more. The evidences show that they are much more in favour of preserving privacy if it's about 'simple' travelling (like using the underground), but when it's more complex (as travelling by plane), they put more emphasis on convenience – and security. For example, the majority of the group (19 participants) would

never use his/ her fingerprints for identification and paying the tickets in the underground, and only the half of this ratio (10 participants) would reject to give up some parts of his/ her privacy for a more convenient check-in or travelling. A reason for this can be that airports have been already more 'technology oriented' – when passengers cannot choose to use these technologies if they want to travel – than stations of public transport, so it can be more accepted at the airports as they have already given up a part of their privacy there.

At the subway, the majority (13 persons) of the people who could accept using fingerprints for identification (15 persons) would imagine it only if it's not exclusive and they can pay in an alternative way. 9 of them would use fingerprints if it's deleted immediately after they paid the fee, and only a few persons (2 and 1 person) would use 'real' fingerprints and accept the reservation of their fingerprints or the template of it in return for convenient travelling in the underground.

It would have been interesting to compare if there is any difference in the opinions according to the frequency of travelling, but as only 5 people don't use public transportation often and 29 travel by it at least once a day we'll leave it out of consideration now.

The second dilemma of convenience and privacy was whether they accept special scanning methods at the airport just for a faster and easier check-in. Although, nearly one third rejected all the technologies listed in the questionnaire, the majority (20 people) of the remaining part (23 persons) would accept the most 'drastic' method: going through the so-called naked machine that shows everything under the clothes. Also a modest majority (14 participants) of this group would accept being thoroughly checked and registered in a permanent airport security database, and then using biometrics for authentication on all further occasions – making travelling more convenient by this. Only 7 would accept being scanned for body heat, sweat and heart rate for the same purpose. Unfortunately, we cannot compare the opinions of those who travel by plane more often with those who don't as only 5 participants out of the 34 take a flight at least once a year.

At the group discussion they also expressed that more convenient travelling was substantial in itself, but they didn't find it really necessary at public transportation. It's also true that giving fingerprints can make travelling less convenient than showing a ticket to the driver or controller when getting on the bus. Another thing was that paying with fingerprints can endanger the money placed on the bank accounts.

> *I wouldn't really give my fingerprints, my daily business might be removed from my bank account. This mistake can happen.*

There were also some special angles that can be worth to think about.

> *These naked machines at travelling are positive for me. It doesn't disturb me, rather saves me from a lot of inconvenience, because there are metal pieces in my body. And when I go to the court, it signals everywhere, and I take the medical certificate with me, the radiograph to prove that yes, these are really inside me and will remain there. … It also disturbed me when I did sport and travelled to abroad, although, we used V.I.P. class, it always 'beeped' and I had to explain it while nearly 600 people were watching at me. I'm happy with this.*

As it was mentioned at the lecture, this technology (iris recognition – E.B.) may harm the eyes of people suffering of diabetes, and my husband has this illness which can result blindness. So I totally reject it.

3.2 Prevention of terror

The second dilemma the participants had to deal with was about preventing terrorist attacks on the one hand, and violating privacy on the other, although, it's not proved if these technologies have a real effect in preventing terrorism. About active CCTV cameras and automatic face recognition, the participants didn't reject the use of this technology (only 3 of the 34 persons, and 2 couldn't decide) because it's privacy infringing and not sure that prevents terrorist actions, but they were worrying much more about false identification of innocent people as terrorists. That's why they rejected the application of this technology not only when it's indifferent that in how many cases the technology fails, but also when it works with a low rate of making mistakes (only 3 persons would accept this last option). The majority (20 out of the 34) would support this technology for preventing terror if only it never makes a mistake and any innocent person is identified as terrorist. A bit less but also some participants (16 persons) would prefer to give up a part of their privacy in frequented places where the rate of crimes is high and terrorist attacks may happen. The scepticism towards the security technologies' role in preventing terror was also emerged in the group discussion.

The amount of data collected about me is not proportional to the security I enjoy in return for it. It doesn't work like this. The terrorist will hide himself the most. …

People can be monitored, but the terrorist works only one time: explodes himself and that's it. How do you know that I'm not a terrorist? I can blow up myself any time. …

At those terror attacks, there were a huge number of those who lived there for 10-20 years, in the community, and their neighbours wouldn't think they could tear off even a piece of grass, but in contrast to it, they could or could have killed people.

They also emphasized that CCTV cameras and face recognition could not really prevent the terrorist action, but rather useful for investigation after it, and could be efficient against 'everyday crimes'.

What will the camera solve? They can watch that the bag exploded. But what will it solve? They cannot obviate it. The man may be arrested.

I live in the 8th district (it's said to be one of the worst district of Budapest regarding the statistics of crime – E.B.), and since there are cameras everywhere no people have been attacked, and the whole place is more secure. There are no burglary, much safer, and it's showed by the statistics.

Since CCTV cameras have been introduced – I live in an 'exotic' place, at the Havanna settlement (this part of the city has a low social status, poor and far from the centre with block houses built in the 'Soviet times' – E.B.), and that's a fact that the number of burglary thefts, car break-ins and senseless injuries decreased. There are still some, but much less. … but it has to know that the criminals there are not 'sophisticated'.

Participants were less supportive towards security technologies in preventing terror if they would be monitored not in public places – i.e. by CCTV cameras –, but in their private sphere. When they were asked whether scanning of personal communication (via telephone and the Internet) could help the police in investigating and preventing terrorist actions in the 'planning phase' but only by watching everybody's communication, nearly one third of the group (9 persons) totally rejected the possibility to let the police to search and combine these data (and 2 couldn't answer) – especially those who use e-mail and Internet often than the others. Those who would accept this procedure mostly (18 participants) preferred to give the police only anonymous communication data, and let them to identify persons only by court order. One quarter of the group (8 persons) wouldn't have problem with the fact that the police could search and combine all databases without any limitation.

> *The problem is that terrorists also know it and try to avoid it. If we take the 11th September, the four terrorists never used mobile phones and didn't write e-mails to each other.*

3.3 Locating of cars and movements

The third dilemma the participants had to face with was about locating cars in case of emergency, or for security reasons – preventing terror attacks, finding stolen vehicles – if it results the infringement of privacy by the possibility of locating all cars' movements. Two thirds of the group preferred personal privacy in this case, and agreed on that installing of eCall system into cars should be voluntary. Half of the group would support the use of this technology in case of serious events or reasons: 15 would accept if the police can switch on the equipment if necessary to prevent criminal or terrorist actions, and 15 persons would accept to use eCall only to ask for help in case of an accident.

The group (29 and 31 out of the 34) rejected the possibility to be registered at any time, or to use this technology for penalizing (i.e. giving speeding tickets, so the equipment should be always activated again).

The answers were very diverse if we take into consideration whether the participants use a car at least once a day or not. On the one hand, those who use a car rarely would accept more the security reason: to let the police activate eCall to find a car if necessary to prevent crime or terror, and also they would accept more if eCall is always activated to give speeding tickets. But on the other hand, these were also those (who use cars rarely) who emphasized that eCall shouldn't be used for any other reason than ask for help if an accident happens. Similarly, those who drive every day preferred more if their car's movement can be located, so security is a priority, but in the same time they also preferred more if installing of eCall is optional, so here privacy got a priority in contrast to security. These contradictions could happen because we focused on whether the participants use a car more often or rarely, but maybe the significant difference does not exist between these two groups but between those who use cars and who don't use at all. Unfortunately, this sample is too small to make remarkable conclusions.

3.4 Privacy enhancing for all

The fourth dilemma the participants were asked about dealt with the importance of privacy enhancing technologies (PETs) to preserve ordinary people's private sphere despite that it also gives the possibility for criminals to be hidden. The group was very much in favour of the priority of privacy in contrast to security of the society: only 3 persons of the 34 said they

wouldn't have accepted any PETs if these technologies might hinder the police to prevent or investigate criminal or terrorist actions. However, we also have to add that one sixth (6 persons) of the group couldn't answer this question at all. Those who accepted some risks for the society (25 persons) with the use of PETs mostly (21 participants) supported the opportunity of encryption, even if it makes difficult for the police to prevent or investigate crimes and terror attacks. Anonymous calling cards were a bit less popular, but also some of the participants (13) would accept it. Internet anonymity was the least preferred option, especially, when it comes to hindering of investigating child pornography (only 3 people chose it). It was also rejected (accepted by 8 persons) when police may be hindered in finding people who read bomb instructions on the Internet.

3.5 Consequences for others

The last dilemma of the conflict between security and privacy was about the consequences of the case if there are effective security technologies to secure the society, but some people cannot use them or simply don't want to use them because of privacy reasons. The majority of the group couldn't accept any negative consequence or disadvantage for people who refuse to use a given technology (21 participants) or for those who are unable to use them (20). Only a few people could imagine that the refusers or unabled are excluded from using some public services (3-3 persons), or to be impeded in some ways when travelling by public transport (4 and 2 persons). It also shows that the participants gave a high priority for preserving privacy that they didn't make a difference whether somebody is unable to use a technology or simply doesn't want.

> *The more a technology is developed, it's not sure that the more people can reach a level to be able to use it. And it's a big problem, because the question was exactly, what should be done. It should be tried to teach to use it.*

Chapter 4 Democratic issues

4.1 Democracy and participation

After reviewing the security technologies and the dilemmas these imply in relation to privacy, the participants had to think about who should be asked when deciding about these questions. In general, they preferred very much to ask the citizens, which technologies and how should be used when politicians were mentioned in the question. One reason for this may be a basic disapproval of high politics and politicians by the everyday people, especially nowadays in the Central European region. Nearly the whole group would give a strong position in discussing and deciding about this subject to themselves: 30 out of the 34 agreed that politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies. And only 3 of them accepted another statement that says: the subject of security and privacy is so complicated that it makes no sense to include the general public in discussions of this issue. Although, this latter question divided the group more than the previous one: 24 of the 34 disagreed on the statement, and 7 couldn't decide.

> *In my opinion it's an important thing that my own security hasn't to be defined by somebody else, but by myself whether I'm under cover or not.*

In contrast, when citizens' role in discussion and decision-making about these matters was not in relation to politicians, but to security and/ or privacy experts, the participants preferred to give a more slightly importance to the general public and everyday people.

> *Scientists who can explain it well, understandably for the average people. Not the politicians, … People should be also asked, but it's impossible to ask everybody. But they must be informed. …*
>
> *In my opinion, if these are applied for everybody, then there should be a referendum whether we want it.*
>
> *A referendum wouldn't have too much sense, because it would be politicized again.*
>
> *People have to be informed correctly, but not asked for their opinions.*
>
> *Not the politicians should make the decisions. …*
>
> *Definitely, the experts.*
>
> *The experts have to be listened to and it should be taken into consideration what they confirmedly say.*

The human rights organisations also got high priority in being involved into the debates on security and privacy – as it's also out of the sphere of politics and closer to the citizens and the civil society. 31 of the 34 participants agreed on the statement that human rights organisations are always entitled to be heard when important decisions on security and privacy are made, but we have to add that these organisations don't have significant positions and effects in

Hungarian politics and public debates as average citizens and sometimes the decisions-makers don't know either them or their arguments.

Opinions about the role of private companies that produce security technologies were much more complex and nuanced than about human rights organisations. It also means that the group was much more divided whether these companies should be asked when deciding about the implementation of security technologies and the consequences to privacy. Approximately one third of the group supported the opinion that it's important that private companies involved in producing security technologies are also entitled to be heard when important decisions on security and privacy are made. Nearly half of the group (15 persons) couldn't decide if it was desirable or not, and some (6 participants) rejected to give an important role to businessmen in the field of security technologies. The participants accepted the argument that the opinions of these entrepreneurs can be important as they know these technologies and producing considerations well, but they also emphasized the importance of being sceptical with them as these businessmen and companies have real, economic interests – not certainly focusing on privacy problems and consequences.

> *It also improves industrial production.*
>
> *But the developers of the technology have also material interests.*

They also mentioned the confusing pattern or ambiguity of high politics for citizens, the relations between politics and financial-industrial lobbies, and corruption as well. There was also an interesting suggestion: to test these technologies before use, and not on average people, but on the members of parliament.

> *But here too, it's also a dangerous thing which has been mentioned here that money matters so much. So, if somebody's interest is that something should be in this way, then s/he'll pay the experts who will say that it should be in that way. … money rules …, that's why I'm very uncertain who's right. So, there is uncertainty.*
>
> *They should develop, make researches and test it on the parliament, and if they accept them, then these will be good also for us. Decisions should be made by politicians and not by experts, security experts. I don't think there are too many MPs out of the something 380 who has much idea about it. They want to influence the decisions-makers by money and technology, so it's not sure that it's the technology implemented at the airport, the bus station, at mobile communication which serves my interest, but to which the slush-fund was given.*

Again, the whole group agreed on that information has to be fully balanced regarding the different options when choosing between security technologies. Although, it's not surprising that people ask for taking into consideration if there is an alternative when making important decisions, it may also show that people feel it to be important as they are not satisfied with the present public debates or decisions, and that's why it can become a 'topic'. 33 of the 34 participants supported the suggestion that in relation to significant decisions on the use of security technologies, it is imperative that alternative solutions are elucidated and included in the debate. At the group discussion they referred explicitly to the dissatisfaction about being informed properly.

> *Citizens' opinion is very important.*

Yes, but they should be informed, because in my opinion, a lot of people don't understand for sure, what is it about, so how are these security technologies. I don't know who should be asked, but if everybody, it would make a huge chaos.

They should be asked and showed alternatives, not only one side of security. … It's related to security that we are a member of the NATO, we shouldn't be. We got information for a long time to be a member, because it's a good thing. And we didn't get counter-opinions. The same happened about the European Union.

These things are more complicated, it's not only about security technology. Essentially, we are lagging behind so much in practising democracy.

But, excuse me, and what about the whole world, also Europe and America?

4.2 Proposals

At the end, the participants had to deal with some proposals how to go on with the researches, introduction and application of new security technologies in relation to privacy infringement. The evidences show that people are worried about monitoring all persons by the authorities, but they are much more worried about misuse of collected data by the organisations and authorities.

The four proposals listed in the questionnaire got very strong support from the participants: the majority of the group gave high importance for them, but it's not surprising as these statements as very 'citizen-friendly'. Although, it's interesting which proposal got higher or lower preference. The one that gained sympathy of nearly the whole group (32 out of the 34 said it to be highly important, and the 2 others gave it some importance) suggested that only authorized personnel shall have access to collected personal data. The other proposal that gained significant support (30 found it very important, 3 moderately important and 1 slightly important) said to be prior to implementing that new security technologies must have been checked for privacy impact.

The other two proposals got lower support, but still the absolute majority gave high priority for them. 27 of the 34 participants found it very important to keep in mind that collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order. Maybe, because scientific researches usually less well-known, the least preferred (24 out of the 34 gave high importance for it) suggestion was that funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts.

Proposal	High importance	Some importance	Little importance	Not important	D.K.
Collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order	27	3	2	1	1
Only authorized personnel shall have access to collected personal data	32	2	0	0	0
Prior to implementing, new security technologies must be checked for privacy impact	30	3	1	0	0
Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts	24	6	1	1	2

There were some participants who made own suggestions at the end of the questionnaire. These are listed in Annex 7, chapter 6.1.7.

Chapter 5 Additional information

5.1 Impact of the event on the participants' attitudes

Finally, there were some comments or perspectives that we haven't touched yet in our analysis so far. The first thing that mostly all groups talked about was the process how they dealt with serious questions that usually never thought about before. In general, they referred to the growing anxiety, worry and fear about security technologies when they became more conscious about the subject after reading, hearing and talking about it. On the one hand, they said they worried much more after the group meeting as they realized that world was so dangerous and there were a lot of risks in many fields of life that they hadn't thought about or realized before. On the other hand, the participants also became more worried because of the privacy consequences of using security technologies in day-to-day life in a society per se, and also when these technologies are misused or used for another purpose than originally introduced for.

> *I never took care in which places I was monitored. It's true from the case of phone calls till the shopping malls, so anywhere I went to. But now, now I thought about it a bit that in fact, we are under control. In spite of the fact that we are not criminals, terrorists, etc., I have to keep it in mind. But it's no matter if I consider it or not, it will happen. So, it's not up to me. And if I allow it or not, it happens.*
>
> *It's a technical thing and a business, big business of big men. I don't like it and I don't feel to be secure. …*
>
> *I have become a bit more frightened.*
>
> *My opinion has changed in the sense that it opened up my eyes a bit that, I don't know but, these matters are really very important and a lot of people don't take care of them.*
>
> *I am frightened a bit more, I will keep these in mind more.*

Another tendency was also possible to be noticed. Some participants mentioned that – like what we described above – they hadn't really taken into consideration how important security technologies could be and for what other reasons (next to security) these could be useful, but after they had got a closer look into this field and the possible counter-effects and privacy consequences by reading the scenarios, they became frightened that there is much more danger also from the criminals' and terrorists' side, and from the authorities' side onto their everyday life than what they had expected before. But, they also added that after listening the expert's lecture and discussing the subject in a small group while they could learn what other 'normal', non-expert, average people think and know about it, they could understand and interpret more about the advantages and disadvantages of new security technologies, and finally, at the end of the day (and the meeting) they became more calm and felt much better. It may also imply that the participants' first impression about the scenarios was rather diffuse and confusing for them, and they were a bit frightened about how dangerous life is in a globalized world, and on the other hand, how dehumanized the everyday life will be with a lot of technical equipments and while being monitored all the time. But at the meeting they faced the possibility of discussing and deciding about their future, or at least, the situation written in the scenarios are not

certainly occurs in the near future. Thus, after having more information, more details about advantages and disadvantages, discussing and arguing with other group members they worried less than after reading the scenarios.

> *My attitudes have changed in the sense that now I see the whole issue clearly, everything, together. Because in fact, one can hear a lot of different things, so even about this. But not that summarized and elaborated like here. People are afraid less of things they know better than of those that are unknown, and it's like this for everybody. From this point of view, it was very useful.*

> *I was also frightened first time, but it's passed away.*

Regarding the numbers, half of the group (16 participants) answered that their attitudes didn't change towards security technologies during the completing of the questionnaire, and two thirds of the remaining part (11 persons) had more worried, one third (7 persons) more posotove feelings.

We also have to add, that there was no problem for the participants to interpret the scenarios, they understood the main issues and dilemmas, and they also explained at the group discussion that they had no problem with them.

Some pointed out that life will be futuristic or as if we were in a sci-fi film when everybody has a chip under his/ her skin. But also some participants emphasized that their attitudes didn't change during the meeting. Either because they had a rather fatalist point of view and couldn't imagine at all that they could be convinced, or because they have a strong believe in the unstoppable nature of technical development and that the world always progresses.

> *I like to feel to be secured. I agree with these improvements of security technologies. We should go further, not backward, after all.*

5.2 Role of the different actors

Some of them mentioned the role of high politics, international organisations and the states in achieving security that is as important as or even more important than technical equipments. These institutions, they argued, have to abolish the basis of crime and terrorism to secure the people and to induce social trust and a general cooperative feeling in the societies.

Another perspective that the participants involved into the discussion was the method how citizens could be informed about new security technologies and the dilemmas these technologies may imply. More participants mentioned they would prefer a regular TV programme that could explain this whole issue, highlighting the different approaches, advantages, disadvantages and consequences as they had the impression that there's no forum for them to look after and know more about it in a 'citizen-friendly' way and language. They also suggested setting up a phone number which they can call during or after the programme if they have questions or comments, or they just have specific problems in relation to the subject. Another thing they urged is to incorporate this issue into the educational system or curricula. They argued that these would be very useful and practical things that every citizen should have known and also to be aware of the privacy consequences to be able to decide whether to use it or not.

> *It should be integrated somehow into the education, this whole issue so that people have clue about it. And also from the point of view of elderly people, the important things that have an impact on them shouldn't be written with microscopic letters in the contracts that they cannot even read.*

And finally, nothing special occurred during the interview meeting that could influence the participants, they haven't mentioned any news events that would have caught their imagination before the meeting and which would have made special implications or views about the subject, other than in the PRISE project.

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 and interview guide
- Annex 5 - Transcript of group interviews
- Annex 6 - Frequency tables
- Annex 7 - Comments from the questionnaire