View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by OAR@UM

Beliefs and attitudes of citizens in Slovakia towards smart surveillance and privacy

Noellie Brockdorff[1], Natalie Mundle[1], Christine Garzia[1], Dusan Soltes[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] e-Europe Research & Development Centre, Comenius University, Bratislava, Slovakia

December 2013

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

SMART
Scalable Measures for Automated Recognition Technologies (G.A. 267127).
The project was co-financed by the European Union within the Seventh Framework Programme (2007-2013).
https://www.smartsurveillance.eu/

The views expressed in this report are the sole responsibility of the authors
and do not necessarily reflect the views of the European Union

Correspondence about this report should be addressed to
Noellie Brockdorff, Department of Cognitive Science, University of Malta, Msida, MSD2080, Malta
noellie.brockdorff@um.edu.mt

Table of Contents

1. Key Findings 3
2. Introduction 5
3. Methodology 6
   - 3.1 Recruitment process 6
   - 3.2 Discussion guidelines 7
   - 3.3 Focus group procedure 7
   - 3.4 Data analysis 8
4. Description of the sample 9
   - 4.1 Composition of the groups 9
   - 4.2 Description of the groups 9
5. Results 10
   - 5.1 Surveillance Technologies in Different Spaces 10
     - 5.1.1 Commercial space 10
     - 5.1.2 Boundary space 11
     - 5.1.3 Common public spaces 12
     - 5.1.4 Mobile devices and virtual spaces 12
   - 5.2 Perceptions & attitudes towards smart surveillance and integrated dataveillance 14
     - 5.2.1 Feelings 14
     - 5.2.2 Behavourial intentions 15
     - 5.2.3 Beliefs 15
       - 5.2.3.1 Likelihood of smart surveillance and integrated dataveillance 15
       - 5.2.3.2 Perceived effectiveness of smart technologies and dataveillance 17
   - 5.3 Security-Privacy Trade-Offs 19
     - 5.3.1 Acceptance of technological surveillance 19
     - 5.3.2 Perception of different technologies 21
   - 5.4 Surveillance Laws & Regulations 23
     - 5.4.1 A lack of information and transparency 23
     - 5.4.2 Trust in the state and effectiveness of legislation 23
     - 5.4.3 Length of data storage and accessibility 24
     - 5.4.4 Data sharing between different actors 24
6. Conclusion 26

Acknowledgements 28

Appendices

A. Recruitment questionnaire 29
B. Interview guidelines (English) 30
C. Interview guidelines (Slovak) 40
D. Debriefing form 48
E. Consent form 50
F. Coding map 52

1. Key Findings

This document presents the Slovakian results of a qualitative study undertaken as part of the SMART project – "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727). The analysis and results are based on a set of three focus group discussions comprising of 33 participants, which were held in order to examine the beliefs and attitudes of citizens towards smart surveillance and privacy.

The focus group discussions were conducted in line with a discussion guide mainly consisting of different scenarios aimed at stimulating a discussion amongst the participants. While some scenarios dealt with surveillance in everyday contexts likely to be encountered by research participants, other scenarios were hypothetical in nature and their aim was to elicit the feelings, beliefs and attitudes of the participants in relation to dataveillance, the massive integration of data from different sources and the "security versus privacy trade-off".

The Slovak participants were in general highly aware of being under surveillance in different spaces including the commercial, boundary and public spaces. Participants mentioned a wide range of surveillance technologies and methods pertaining to different spaces, including the use of loyalty cards to monitor customer behaviour and the use of CCTV systems for the observation of citizens particularly in boundary and public spaces. Overall, participants perceived that customer surveillance takes place for marketing and advertisement purposes, while general citizen surveillance occurs for reasons of national security. Nevertheless, although many participants showed a general acceptance towards data collection for such purposes, some participants expressed concern in relation to how their data might be used and disseminated.

In order to gauge participants' attitudes and beliefs on dataveillance, the group was presented with a fictional scenario illustrating the massive integration of data. After an initial intense reaction to this situation, the participants debated the possibility of dataveillance and massive integration of personal data taking place and proceeded to differentiate between technical and ethical aspects. Even though in comparison to other countries the participants believed that Slovakia's technical capacities in this field were less developed, the massive integration of data was still perceived as being possible. On the other hand, from an ethical point of view, most participants were principally against extensive integration of data from dataveillance mostly since this was perceived as presenting an invasion of privacy to citizens.

With regards to the understanding of technology-mediated surveillance, it appears that participants found surveillance methods involving the integration of data from different databases (dataveillance) easier to understand than surveillance which is automated in nature (smart surveillance), in particular in relation to autonomous decision-making processes without human influence. Participants' opinions differed in relation to the effectiveness of this automatic process. While some participants argued that the absence of a human operator in the decision-making process was perceived as eliminating

subjectivity and also of decreasing the risk of data misuse, other participants expressed concern that an autonomous process could lead to potential errors.

During the discussion of the “security-privacy trade off” scenario, the results indicate that for the majority of participants, the scenario was considered as unacceptable and extreme. Rather than enhancing feelings of personal safety, for some participants the security measures portrayed in this scenario resulted in feelings of deep insecurity and vulnerability. Moreover, some participants doubted and challenged the notion that surveillance presents the best solution for the reduction or elimination of crime. Nevertheless, a minority of participants were less disturbed and stated their willingness to sacrifice their privacy in order to feel safe, perceiving surveillance as effective for crime prevention.

With reference to the participants’ perceptions of a number of surveillance technologies, the different types mentioned in the scenario seemed to meet different levels of acceptance. Overall, while most participants expressed their acceptance of CCTV systems, ANPR and sound sensors, the use of biometric technologies and location tracking technologies such as electronic tagging provoked in the participants strong resistance. Rather than increasing feelings of safety, these surveillance practices caused uneasiness and a heightened sense of vulnerability amongst the majority of participants, who not only felt a strong invasion of privacy but also a loss of control.

Finally, participants underscored their limited knowledge of privacy laws and regulations. Despite such lack of knowledge, opposing views of the effectiveness of legislation was evident; while some participants regarded current legislation as ineffective and untrustworthy, others were satisfied with and displayed trust in privacy laws. Additionally, in relation to the length of storage of surveillance data, the more private the data was considered to be, the more issues of data storage became subject to debate. Lastly, the sharing of data was in general regarded negatively, mostly due to the perception that this practice could possibly result in a higher risk of misuse, especially when such sharing occurred between private entities.

2. Introduction

The analyses and results in this document are based on a set of three focus groups carried out in order to gauge the attitudes of citizens towards smart surveillance and privacy. This research was undertaken as part of the SMART[1] project.

The University of Malta as Work Package Coordinator was responsible for the design of the research materials, methodology, and coordination between partners, data analysis and report writing. The SMART project partners in each country were responsible for the translation and back-translation of the research materials, recruitment of participants, recruitment and briefing of moderators, conducting the focus groups, transcription of the discussions, and translation of transcripts into English. The SMART project partner for Slovakia is Univerzita Komenského v Bratislave (FMUNIBA).

Focus group discussions were conducted in a total of 14 countries and this document provides the findings from the study that are relevant to Slovakia. Other separate reports are available for Austria, Bulgaria, Czech Republic, France, Germany, Italy, Malta, Norway, Romania, Slovenia, Spain, the Netherlands and the United Kingdom.

The following table provides a breakdown of the participants according to country, age and gender:

Country	Group 1 (18-24 years)		Group 2 (25-44 years)		Group 3 (45+ years)	
	M	F	M	F	M	F
Austria	2	4	3	4	4	2
Bulgaria	6	6	5	5	2	6
Czech Republic	4	6	4	5	4	5
France	5	4	5	4	5	5
Germany	1	6	4	3	4	4
Italy	1	5	3	3	2	7
Malta	5	5	4	6	3	5
Norway	3	6	4	3	2	5
Romania	6	1	3	4	2	4
Slovakia	7	6	5	5	5	5
Slovenia	5	5	5	3	6	4
Spain	6	5	6	3	3	5
the Netherlands	2	4	6	2	4	4
United Kingdom	4	2	5	3	5	4
Sub-total	57	65	62	53	51	65
Total	**122**		**115**		**116**	

[1] "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727) – which was co-financed by the European Union under the Seventh Framework Programme for Research and Technological Development of the European Union (SEC-2010-6.5-2. "Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules").

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research. All 42 groups had between 6 and 10 participants, excluding 3 groups which had 11, 12 and 13 participants respectively. The focus groups in Slovakia were carried out on the 18th February, 2013; 20th February, 2013 and 25th March, 2013. More information on the composition of the group is provided in Section 4.

Personal references and snowball techniques were used in order to recruit participants willing to take part in this study which does not claim to be necessarily representative for the entire EU population or any of the individual EU countries where focus groups were conducted.

3.1 Recruitment process

As illustrated in the table above, three focus groups were conducted in each country which were composed of participants from the following age groups:

- Group 1: 18-24 years
- Group 2: 25-44 years
- Group 3: 45+ years

A number of selection criteria were recommended with regards to the recruitment of the focus group participants and therefore all potential participants were asked to fill in a recruitment questionnaire (see Appendix A). While the recruitment of an equal number of males and females was recommended, it was also desirable to recruit participants with a diverse educational level and occupational status. Effort was also made in order to recruit participants residing in different locations (city, town and rural area). Moreover, in order to be recruited, it was suggested that participants should be exposed to a number of surveillance applications and technologies in their everyday life. Although such recommendations were suggested, the fulfillment of all these criteria proved rather challenging during the recruitment process.

It should also be noted that during the recruitment process, potential participants were not provided with detailed information about the topic of the focus group. They were solely told that the discussion would be on the topic of "technology and privacy". This was done in order not to influence or bias the discussion.

The recruitment process in Slovakia was problematic as most people invited to participate had concerns about the protection of their identity. Although they were told that they would not be identified in any reports and their comments would be linked to a participant number (not a name), due to the fact that the participants had to sign the consent form using their name they were concerned that it is very easy to link participant numbers with names. Due to this, some participants did not want to be identified

during the discussion by a participant number and were speaking only on condition that there would be no identification of their views at all.

3.2 Discussion guidelines

Discussion guidelines (see Appendix B) were developed with the aim of gauging citizens' awareness and understanding of smart surveillance technologies and also at gaining an in-depth understanding of citizens' beliefs and attitudes towards smart surveillance and privacy. The discussion guidelines were developed and further refined following a pilot study conducted in November 2012. The discussion guidelines were designed to tackle the main themes under study through a variety of scenarios. While some scenarios dealt with surveillance in everyday contexts likely to be encountered by research participants, other scenarios were hypothetical in nature and their aim was to elicit the feelings, beliefs and attitudes of the participants in relation to dataveillance, the massive integration of data from different sources and the "security versus privacy" trade-off.

The discussion guidelines were translated into each national language where the research was conducted. Moreover, back translations were carried out which entailed an independent translation of the discussion guidelines back into English by a different translator. The back translation was then compared with the original version in order to ensure comparability of meaning and clarify any possible discrepancies. Any possible changes were discussed with the partners, and, where relevant, the necessary amendments were carried out until a final version of the discussion guidelines in the national language was approved. The Slovak version of the discussion guidelines can be found in Appendix C.

3.3 Focus group procedure

The focus groups were conducted by a team consisting of a moderator and an assistant moderator. In certain cases, other team members were present in order to assist with logistics and other tasks including taking notes during the discussion and filling-in a de-briefing form (see Appendix D) at the end of each session.

All participants were required to read and sign a consent form (see Appendix E) prior to their participation in this study. The participants were informed that everything that is recorded during the session will be kept confidential and that their identity will remain anonymous. The moderator also informed the participants that they will be assigned a number each and that only this number will be used in the report.

All focus group sessions, which were audio-recorded in order to be transcribed, were conducted in the local language. In general, the duration of the sessions was around one to two hours. Following the end of the session, some partners opted to offer incentives for participation including monetary remuneration or the provision of tokens such as book vouchers. Additionally, those participants who were interested in the research were given more information about the SMART project.

3.4 Data analysis

After conducting the focus groups, all sessions were fully transcribed in the local language and subsequently translated into English. The de-briefing forms were also translated into English. The coding process was carried out by three researchers and was based on 3 different data sets (the English transcripts from Austria, Czech Republic and Italy). An initial coding structure was developed through the process of coding and re-coding as the transcripts were read and interpreted. Such a process initialised a critical recategorising and rethinking of the codes first applied, and allowed for a more focused data analysis and drawing together of overarching themes. Thus, the initial coding map was modified as the analysis unfolded. This process of revision was concluded once no new themes emerged and a final coding map was agreed upon. Nevertheless, the emergence of additional lower order codes was not excluded since the analysis of the remaining transcripts was still pending at this stage. The coding map for this report can be found in Appendix F.

Further to the above process, the researchers proceeded to analyse the remaining 11 data sets. Draft versions of each country report were prepared and provided to the respective partner for revision and amendments.

4. Description of the Sample

4.1 Composition of the groups

The data analysis for Slovakia is based on a total of 33 participants. While Group 2 (25-44 years) and Group 3 (45+ years) each had the maximum suggested amount of participants i.e. 10, in Group 1 (18-24 years) 3 extra participants were recruited amounting to a total of 13 participants.

Regrettably, it is not possible to provide a detailed breakdown of the sample of the Slovakian groups as this was not supplied by our Slovak partner. The research methodology envisaged that participants are each assigned a number (as detailed above in point 3.3); however, it was reported that several participants in Slovakia objected to this. Although in the transcripts a number was assigned to the responses, this number cannot be linked to a particular respondent. Moreover, some of the responses pertaining to the discussions held in Group 2 (25-44 years) and Group 3 (45+ years) are missing a participant number. Due to this, some of the quotes presented in the results section of this report do not specify the participant number but only the group number. In this case, the quotes are only identified by the focus group number.

4.2 Description of the groups

Although there were slight differences in the atmosphere of the three groups, in general the atmosphere was described by the moderators as friendly, cordial and relaxed. Participants in Group 1 (18-24 years) were described as communicating in a rather open manner during the discussion and Group 2 (25-44 years) and Group 3 (45+ years) participants were described as being particularly active.

Some problem areas were noted by the moderators while conducting the focus group discussions. In particular, it appears that Group 1 (18-24 years) participants found difficulty in keeping their concentration as the discussion progressed, whilst Group 3 (45+ years) participants tended to deviate from the topics under discussion.

5. Results

5.1 Surveillance Technologies in Different Spaces

In order to establish what the focus group participants actually knew about different surveillance technologies in different spaces – who is collecting what types of information, where and for what purpose – they were asked to imagine everyday situations like being in a supermarket, in an airport whilst travelling, visiting a museum, participating in a mass event such as a football match or concert, and simply using their mobile phone.

5.1.1 Commercial Space

In the commercial space, specifically in the context of a supermarket, participants in all focus groups generally displayed a high awareness of being surveilled and of having their data collected through different means including financial monitoring, i.e. the surveillance of debit or credit card movements, as well as the use of loyalty cards. Firstly, most participants perceived personal data, such as names and addresses, as primarily being collected for the purpose of creating customer databases, and secondly, they understood data connected to customer buying behaviour being collected for market research and sales optimisation, mainly by supermarkets and marketing companies.

The use of CCTV systems as a means of surveillance in commercial spaces was mentioned only by focus group III members (age 45+) and the major purpose identified in this regard was predominantly the pervasive observation of customer buying behaviour: *"They are monitoring your movements, where you go, or from where you come frequently, or where you walk, how much you spend, what people buy […] they want to know everything about you"* (P1-III). Such close observation was considered as having several objectives, including theft prevention and investigation, mainly in relation to supermarket merchandise. However, rather than regarding such surveillance as protecting the interests of customers, there was a general tendency for participants to perceive the use of surveillance as primarily safeguarding the needs of businesses owners. This gave participants the impression that CCTV was working against them rather than being in place for their security:

> *"From my experience, their [security personnel] job is to protect the goods in the shop and not to watch and protect customers. They therefore do not help those people who suffered some harm in that shop being monitored by CCTV" (P3-III).*

Nevertheless, a minority of participants from focus group 3 did mention the possibility of video recordings being used in order to investigate cases of robbery or theft involving customers and their belongings. Additionally, other reasons mentioned with respect to consumer observation included those relating to marketing and advertising: *"perhaps they need it for promotional campaigns"* (P3-III).

Many participants indicated a general acceptance towards the use of their data for specifically market research purposes and they mentioned a number of benefits. While these advantages were mainly perceived as benefitting the commercial establishment, in certain cases participants also acknowledged benefits for the customers themselves. In particular, participants believed that their data is being used for the customisation of newsletters, leaflets, promotional campaigns and advertisements. In general, such strategies appeared to be received rather positively, especially when the data was used with the intention of enhancing customer service. Additionally, other benefits mentioned included the possibility of an improved product organisation and optimisation of sales.

Nevertheless, participants also expressed a number of concerns about the use of their data and its dissemination after having provided consent to the commercial establishment: "*Hopefully the data is not misused for anything else*" (P7-I). Although participants seemingly expected their consent to be linked to clearly specified conditions of data use and dissemination, they also acknowledged an increasing loss of control: "*We sign and give consent that this confidential information can be used only by this company, but in reality nobody knows where the data ends up and if it is used for other purposes*" (P2-II). Participants expressed their belief that shops use their data mainly *"for [...] their [own] benefits"* (P3-III), and not for the benefit of customers. In particular, a participant expressed concerns regarding the misuse of CCTV as a spying tool by staff on customers: "*Shop workers may require information at any time, without reason. They will say that they feel that someone is stealing and so they can track anyone, any time, for any reason*" (P3-III).

5.1.2 Boundary Space

In the context of border control in spaces such as airports, surveillance and the collection of personal data was perceived as occurring by a variety of ways and means. When entering an airport, participants felt "*monitored right from the start*" (P2-III) by the constant monitoring of CCTV systems, which they regarded as a surveillance device mainly utilised for national security purposes. Additionally, participants also mentioned surveillance via other methods including passport controls, criminal record checks and financial monitoring. Participants perceived these types of personal checks as occurring not only for organisational reasons, security purposes and an improvement of customer service, but also for the creation of databases and statistics, and for marketing purposes.

In addition to the personal data checks mentioned above, participants also mentioned surveillance by object and product detection devices including X-rays and body scanners. The latter technology was particularly perceived as extremely intrusive: "*Let's say that it is not just about monitoring, but about monitoring of your body, when one must stand with the arms and legs straddled and they scan all and can see how the person looks"* (P2-III). In particular, the surveillance measures at foreign airports, especially in the United States, were considered as extreme, especially those which utilise biometric technologies such as the scanning of fingerprints and retinal scans. Some participants stated that such measures present a strong invasion of privacy and, in fact, they expressed their hope that Slovakia would not expand its surveillance measures at airports to such an extent.

On a more general note, it appears that Slovakian participants considered most security controls at airports as extremely intrusive and as representing a threat to privacy. The presence of police and security staff who have been employed in the same positions from before the 1989 change in political system may contribute to these perceptions.

5.1.3 Common Public Spaces

In common public spaces, participants mentioned CCTV as the main instrument utilised for surveillance during mass events or in public spaces such as museums. Participants also mentioned surveillance in potentially sensitive areas such as embassies. In such cases, the majority of participants perceived security reasons as being the main purpose of surveillance. Specific security purposes mentioned by the participants included the prevention of crime: *"To identify possible wrong doers"* (P9-III) as well as crime investigation in case of *"incidents […] to know who started it and to know why it started"* (P11-I). In addition to CCTV, the use of electronic entry gates in certain buildings was also mentioned by the participants in relation to security-related surveillance. In general, such uses of surveillance technologies were regarded rather positively.

Moreover, personal data such as name, surname and age was also perceived as being collected during other occasions, including the purchase of admission tickets. In these cases, participants mentioned various uses for data collection, including the creation of databases, marketing research, and advertising-related uses. Moreover, participants believed their information to be used in order to improve operations as well as customer service and experience in these spaces.

In general, it appears that participants perceived the aforementioned surveillance measures in the public space as justified and hence as acceptable for security reasons as well as for marketing purposes.

5.1.4 Mobile Devices and Virtual Spaces

In relation to surveillance of mobile telecommunication devices and internet activities, participants were aware of being under surveillance through a multitude of ways. This included the monitoring of call lists, text messages and website logs by mobile phone operators. To a lesser extent, participants also mentioned location tracking by GPS, as well as phone tapping. The monitoring measures appeared to be relatively accepted by participants because in their opinion, mobile phone operators were entitled and sometimes even obliged by the legislator to save specific customer data for a limited time period, for reasons pertaining to criminal investigations. In addition to security reasons, marketing and sales purposes were also mentioned by the younger participants.

At the same time, however, participants expressed their fear of data leaks from the computerised systems of mobile phone operators. In this regard, some participants argued that third parties, such as private detectives or even family members, could access such stored personal data by means of special

programs. Due to this perception, a number of participants claimed that they sometimes change their behaviour, such as for instance meeting in person rather than having a phone conversation when discussing *"personal things"* or *"private matters"* (III).

This rather anxious attitude towards surveillance and the intention to prevent or avoid being monitored at times reminded participants of focus group 3 (45+ years) of their experiences under the past socialist regime in Slovakia: "*The regime was monitoring everything about the people, even without the technologies which are available today*" (III). Nevertheless, some participants argued that the fast development of new surveillance technologies made intense surveillance more achievable: "*The possibilities are much better today than before. As we sit here, I see no reason to be monitored, but if they want, they can monitor me 24 hours a day because they now have all necessary technology*" (P1-III).

In the context of virtual spaces, participants from group III (45+) regarded data sharing in virtual spaces as a personal choice, thus linking this to the self-responsibility of the individual. This was especially the case when referring to the use of social networks; these participants seemingly considered themselves as being more aware than younger people about the ever-increasing surveillance possibilities in the virtual space: "*The older generation is more cautious, the younger generation is less cautious, they do not realise the risk they expose themselves to when using [for example] Facebook*" (P1-III). Lastly, to a greater extent, the older participants perceived a systematic collection of their data as occurring when purchasing products and services online. This awareness seems to elicit a certain degree of insecurity due to the evident inability of knowing where their data would end up.

5.2 Perceptions & Attitudes towards Smart Surveillance and Integrated Dataveillance

One of the central tasks of this study was to research citizens' feelings and beliefs on smart surveillance and massively integrated dataveillance, the latter referring to "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons"[2]. In order to tap into the attitudes of the participants, the group was presented with an everyday scenario: a recorded telephone conversation between a job seeker and a civil servant of the employment agency, where complex surveillance[3] becomes evident.

5.2.1 Feelings

After having listened to the recorded conversation, the focus group participants revealed feelings which ranged from 'passive' discomfort, including helplessness and fear, to 'active' anger. A minority of participants additionally reflected on the positive aspects of dataveillance, which will be dealt with later on. Nevertheless, the predominant feeling amongst the different focus groups was an extreme sense of discomfort, with participants feeling "*upset*" (P4-II), "*uncomfortable*" (P3-I), "*terrible*" (P1-II) and *"shocked"* (P6-III).

When confronted with possibilities of dataveillance and the technological progress of surveillance tools, in addition to feeling *"scared"* (P1-II), many participants conveyed an intense feeling of helplessness, which becomes even more evident from the behavioural intentions outlined further below. Upon imagining that their personal data could be available to others, some participants perceived a power imbalance between citizen and state, which ultimately resulted in a feeling that the citizen is no longer in control.

Other stronger feelings were also conveyed; certain participants expressed their indignation and anger, perceiving the scenario as "*disgusting*" (P4-II) and as a threat to their privacy: "*It is a huge intrusion into privacy*" (P6-II). In particular, possible access to both financial data and health data by third parties, coupled with the risk of misuse, was considered as unacceptable and unethical. This was especially the case when private companies were involved, which at times caused feelings of anger: "*I would probably destroy all technology that I have around me*" (II).

In contrast to the above negative feelings, some participants reflected upon the convenient aspects of the integration of different databases. With a specific reference to government services, one participant argued that this would contribute to a more efficient service: "*I see one big advantage; you would not need any more to bring the same paper to 14 offices, but only to one"* (III). Further perceived advantages

[2] Clarke, R. (1997)

[3] The statements of the public servant allude to a drawing together of the job-seeker's personal information from various public and private databases, health-related information, bank / credit card data, surveillance of online social networks, and CCTV. See Appendix B, Item 4 for full text of scenario.

of dataveillance were of a commercial nature; in this case, participants believed that it could enhance personalised offers of products and services by companies. Participants also considered the benefits of shared medical records amongst doctors and health institutions for a more holistic treatment or in possible cases of emergency.

5.2.2 Behavioural Intentions

After listening to the hypothetical recorded telephone conversation between a job seeker and civil servant participants were also asked what they would do if something similar happened to them. Mirroring the predominant feelings of discomfort as described above, the prevalent reaction amongst participants was in general rather passive. The participants mentioned a number of passive and precautionary actions including inertia, engaging in some form of escape from modern society and adjusting their behaviour in order to avoid surveillance. Nevertheless, some participants did express reactions which were of a more 'active' nature.

In general, it appears that those participants who displayed a sense of inertia perceived citizens as being powerless and helpless against 'the system'. These individuals could not conceive of how they could possibly counteract surveillance in its many different forms: "*I would not do anything against it, because it is clear that I have no power to change it*" (P6-I). Similarly, another participant conveyed a deep sense of resignation: "*[…] such systems already exist and we cannot prevent anything about them. We have to live with that. Would it be possible to stop using credit cards? Not really*" (P6-III). Additionally, some participants questioned whether escaping to a remote location would possibly be the only option in order to avoid surveillance: "*Should I go and live on an isolated island*?" (III). Nevertheless, while these participants discussed such a complete disconnection from society, at the same time they acknowledged that this is not a realistic option.

Actions of a precautionary nature were mentioned by a number of participants which mainly targeted a change in behaviour. These included self-censoring and the adoption of a more careful approach when divulging personal information (most notably in relation to online behaviour), paying in cash in order to avoid financial monitoring and reducing the use of mobile phones. In addition, as mentioned earlier, participants also revealed intentions of an active nature, including taking independent action and asking for assistance. While for instance some participants claimed they would hang-up the phone and investigate where their data had been obtained from, others claimed they would investigate the legitimacy of the situation, or try and find other citizens who went through similar experiences.

5.2.3 Beliefs

5.2.3.1 Likelihood of smart surveillance and integrated dataveillance

Regarding the likelihood of whether or not massively integrated dataveillance is possible (currently and/or in the future), the clear majority of the focus group members perceived the use of these

technologies as likely, although some participants did express an initial disbelief at such a scenario: "*I cannot imagine this happening*" (III). Additionally, here some participants alluded at the 'invisibility' surrounding this type of surveillance: "*Yes. It is happening. People just do not realize it*" (III). Along similar lines, another participant stated *"ignorance is bliss. If we do not know that this exists at all, I would not even be bothered by that"* (III).

Some participants of group 3 argued that the intensification of massively integrated dataveillance is spurred by a number of factors. Firstly, they perceived that such intensification is inevitable since citizens are now living in an *"information society"* and hence "*such systems can no longer be avoided"* (III). Secondly, some group 3 participants also mentioned the profitability of surveillance for commercial purposes as leading to further intensification: "*It will always be like that, if it is such a good business and brings in a lot of money*" (III). In relation to this, the perception of surveillance as a profitable business was underlined by participants claiming that, in general, surveillance was not used "*in the interest of the people"* but rather misused *"in the interest of those rich businessmen* […]" (III).

Participants further discussed the likelihood of massively integrated dataveillance according to both technical and ethical aspects. From a technical perspective, participants perceived modern surveillance systems in Slovakia to be sufficiently advanced in order to allow the development of such intrusive surveillance. Nevertheless, in comparison to other countries, they believed that Slovakia's technical capacities in this field were less developed. However, while from a technical perspective such a development was considered as being possible, from an ethical viewpoint most participants expressed a number of reservations. Some participants argued that the acceptance of surveillance in Slovakian society is rather low, a factor which they considered as presenting a likely obstacle to excessive surveillance measures. In particular, covert surveillance was clearly considered as unacceptable amongst a number of participants: "*So why should I be monitored without my knowledge and consent?"* (P10-III).

Overall it appears that most participants were principally against massively integrated dataveillance mostly since this was perceived as presenting an invasion of privacy: *"It is a too big intrusion into privacy [...] The possibility should not be given to other people to know information about me, this data is my private data"* (P6-II) In fact, some group 3 participants questioned whether surveillance measures focus solely on irregularities or are in fact employed in order to monitor every single citizen irrespective of whether such surveillance is justified or not: "*If I behave like a normal citizen and fulfill my duties, tasks and so on, then they should not even notice me, I hope, but who knows?*" (III). In addition to privacy reasons, some older participants were particularly distressed at the thought that in the case of smart surveillance a "machine" could control humans and ultimately society: "*But, should we accept that this machine is God and decides about everything around us?*" (III).

Participants' acceptance of massively integrated dataveillance also depended on the type of data collected and shared. While the collection and sharing of personal data such as name, age and gender was widely accepted, the collection and sharing of other data such as email address, personal tastes and photos was less accepted. Moreover, data considered as most sensitive included financial information,

medical data, and the browsing history of computers. Such information was regarded as extremely confidential and some participants expressed their concern at not knowing where their personal data is ending up. Moreover, another concern mentioned by some of the participants of focus group 3 was the possibility of technical errors, such as the accidental assignment of electronic data of a criminal person to an innocent citizen: "*They might blame me for something which I did not do*" (-III).

5.2.3.2 Perceived effectiveness of smart technologies and dataveillance

When discussing the effectiveness of surveillance technologies, participants mainly differentiated between traditional surveillance technologies, in which case it was perceived that human judgement is necessitated in decision-making, and smart technologies, in which case it was perceived that decisions are taken by a computer programme. In general it can be said that participants encountered a certain difficulty when attempting to understand the operational nature of smart technologies, in particular in relation to the autonomous decision-making processes of these technologies: "*When there are hundreds of people on CCTV, how can a computer find the one person it is looking for, there must be a special program for it, I do not know*" (P5-III).

The automated process by smart surveillance technologies, referred to by one of the participants as a "*special program*" (P5-III), appears to have raised a certain degree of uneasiness and fear in most of the participants. During the discussion, the effectiveness of smart technologies was challenged by the majority of participants. Feelings of apprehension appeared to stem from the belief that wrong conclusions could be potentially drawn during this automatic decision-making process, which consequently would result in an erroneous assessment or interpretation of a given situation. In relation to this, participants perceived smart technologies as lacking the ability to consider all circumstances. These participants appeared to be skeptical and distrustful of technology on its own without human agency, and, accordingly, they argued that the human element is necessary for a correct and complete assessment of a given situation: "*If I drive fast because I have a wounded person in my car, the devices would fail to record the circumstances of my speeding, which should be taken into account*" (P7-II).

Possible errors and misunderstandings were presumed to occur in other ways, for instance in cases where smart systems recognise particular words which are linked to a threat, such as the word '*bomb*'. Participants pointed out the ambiguity of the word, being also used in everyday language as a synonym for an attractive woman. In their opinion, such ambiguities could lead to a wrong conclusion: "*No machine is able to differentiate this difference and they could act against logic in the fight against terrorism*" (P?-III).

An additional concern discussed by the participants was that 'machines' would be programmed for the sole recognition of behavioural patterns which are considered as undesirable or prohibited, which they referred to as "*negative points*" (P2-II). A number of participants perceived such a selective focus as a disadvantage since good behaviour would consequently be disregarded. Moreover, participants imagined these collected "*negative*" or "*minus points*" (P1-II) to be saved and added to their records

which could then be accessed during personal data checks: *"They are collecting information about you which then becomes part of a complex [collection of] information about you*" (P6-III). The creation of such records was perceived as detrimental to citizens given their belief that such a system would keep a record of every single transgression or mistake they did.

In contrast to the above opinions, albeit to a much less extent, some participants expressed a preference for automated decision-making by smart technologies in specific circumstances. Amongst the benefits mentioned by participants was that in certain situations, the absence of a human operator throughout the process was viewed positively in terms of privacy reasons; as stated by one of the participants, "*I would not feel like someone is stalking me"* (P3-I). In addition, a number of participants perceived a substantially lower risk of data misuse due to the automated nature of the process: "*It would be better if computers take decisions […] because there would be less possibility to misuse the data*" (P3-I).

Lastly, another issue in relation to effectiveness was the belief that, in certain cases, the 'objective' judgements taken by automatized systems may present an advantage given that such judgements were considered by some participants as being emotionless and thus as lacking human bias. However, some participants challenged the inherent objectivity of smart systems by arguing that the programming of surveillance technologies incorporates a subjective decision-making process, since, in the end: "*Each machine does what a human wants it to do*" (III).

5.3 Security-Privacy Trade-offs

5.3.1 Acceptance of Technological Surveillance

In order to gauge participants' perceptions vis-à-vis the security-privacy trade off, as well as their attitudes towards a number of specific smart technologies, a hypothetical scenario was presented to the group. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging. The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[4].

When discussing the scenario, the participants' reactions were rather mixed. It seems that while the majority of participants revealed an intense negative reaction to the scenario and considered it as unacceptable and extreme, other participants were less disturbed and stated their willingness to sacrifice their privacy in order to feel safe. Additionally, a minority of participants were rather hesitant and expressed a certain level of ambivalence: "*I really do not know which of these technologies are acceptable or not*" (III).

Participants from the different groups put forward several reasons as to why the use of several smart technologies would be unacceptable. Rather than enhancing feelings of personal safety, the security measures portrayed in this scenario resulted in feelings of deep insecurity and vulnerability in some participants. In addition to reactions of uneasiness, cynical reactions were expressed by some of the older participants who had experienced a socialist political system: "*This [surveillance] is for your safety? Ha-ha*" (P10-II).

One major concern relates to privacy, considered by some respondents as being *"a fundamental human right"* (II), were brought up. A number of participants perceived that surveillance tools could potentially be employed for the unjustified monitoring of citizens: "*They [the state] would know everything about criminals, but not only. They would know everything about me as well"* (P7-I). Nevertheless, some participants argued that law-abiding citizens need not be worried by such technological surveillance: "*Well, I know that it can sometimes turn against people, but if you live normally, then you do not need to be worried about any monitoring*" (III).

The threat of data misuse by the state was a further concern expressed by a number of respondents: "*I would not feel safe in any of the scenarios, because collected data can be misused. Yes, I would feel vulnerable. I would not sacrifice my privacy in any case*" (P8-I). Additionally, some respondents argued that surveillance tools or measures could be misused by criminals who might take advantage of possible

[4] The full scenario can be found in Appendix B, Item 5.

technical flaws since it was perceived that "*every software has its own weaknesses"* (P1-II). Therefore, technological progress itself was seen as providing criminals with more access to sensitive information and with new ways and possibilities of misappropriating data. Consequently, in light of such risks, several participants questioned whether the use of surveillance would indeed create a safer society: "*Who has information can use it and benefit from it. And then he can manipulate the whole society. This would not increase the general security*" (III).

This leads us to the second major reason as to why the extensive use of smart surveillance as described in the hypothetical scenario was considered as generally unacceptable. As illustrated by the preceding quote, several participants raised concerns regarding the possible manipulation and control not only over citizens, but also of society. As stated by another participants, "*in my opinion we would be slaves of this whole system*" (P10-II). Furthermore, the thought of an extreme and rapid intensification of surveillance measures presented further concerns in relation to control:

> "*Very soon everyone and every animal will have a chip installed and be controlled permanently. GPS systems are already used which can monitor the whole globe. [...] I only hope it will not reach a state where they can also control our brains (III).*

In line with the above-mentioned reservations, a number of participants doubted and challenged the notion that surveillance is the best solution to reduce or eliminate crime, arguing that other methods should be actively considered: "*To fight criminality there are many other ways that are more effective*" (P12-I). However, these participants failed to clearly specify the nature of the alternative methods alluded to. Doubts were also expressed in relation to the effectiveness of technologically-mediated surveillance in the investigation of crimes: "[...] *they often say that on the basis of the records from bank robberies, they cannot even identify who the criminals are*" (P6-III). On a more general note, in addition to the use of surveillance for crime investigation, some participants seemingly implied that, in part, the effectiveness of smart technologies rests with providing some sort of advantage to the citizen and to society; as stated by one of the participants, "the question is if this technology is able to help us" (P5-III).

Nevertheless, a minority of participants did argue in favour of the deterrent effect of surveillance; these participants perceived surveillance as a supportive element in the reduction of crime since they argued that individuals would avoid engaging in misconduct due to possible repercussions: "*When there are camera systems on public transport there are less destroyed buses, because people are afraid to damage something as everything can be recorded*" (III).

On the other hand, when participants were confronted with a significantly increasing crime rate in the alternative versions of the original scenario, some participants claimed that the discomfort of being surveilled would be acceptable as long as crime was prevented and safety increased. Therefore, confronted with a higher crime rate, participants showed their readiness to trade their privacy for the sake of increasing safety: "*I would feel safe. [...] Prevention is good. I would accept such use of technology in case there is a proven threat to fight against*" (P2-I). Whilst the tracking of individuals was in general

considered as not acceptable, the use of surveillance for the tracking of missing people was regarded positively since in such cases, "*someone's life can be saved*" (P10-II).

With regards to locations of deployment of surveillance technologies some general observations can be drawn. Surveillance was considered as generally acceptable in public places such as shopping malls and parks, as well as in places considered as high risk areas, such as airports. Moreover, it seems that participants showed a higher acceptance for the monitoring of larger crowds since it appears that they perceived themselves as being less identifiable in such a context. Nevertheless, there was a minority of participants who did object to being monitored in public spaces. Lastly, surveillance was considered as unacceptable in private spaces, mainly in homes.

5.3.2 Perception of Different Technologies

Overall, different types of surveillance technologies seemed to meet different levels of acceptance. In general, whilst the majority of participants expressed their acceptance for CCTV, ANPR and sound sensors, biometric technologies and location tracking technologies such as electronic tagging provoked a strong feeling of violation of privacy among participants.

In relation to video-surveillance systems, the use of CCTV was considered as generally acceptable especially for reasons of security. Such acceptance was however contingent on whether certain private spheres are respected, as already mentioned in the previous section. However, when it came to such use in commercial spaces, a number of participants showed a certain level of mistrust and scepticism. Recounting their experiences, some participants perceived video-surveillance systems as being utilised exclusively for the benefit of the commercial enterprise: *"[...] they [CCTV systems] do not really protect the customers. For them, it is completely useless"* (P8-III).

Sound sensors seemed to be widely accepted by participants of group I (18-24 years), but participants of focus group III (45+ years) showed their discomfort regarding possible wrong conclusions which could be drawn when one simply behaved noisily in the streets: "*So if I sing on the street just because I'm happy it will also be recorded although it has nothing to do with any wrong doing*" (III).

The collection of biometric data and electronic tagging brought about the most negative reactions from the participants in all groups. Rather than increasing feelings of safety, these surveillance practices caused uneasiness and a heightened sense of vulnerability amongst the majority of participants, who not only felt a strong invasion of privacy but also a loss of control. Some participants reacted strongly at the possibility of this type of surveillance, at times in a rather sardonic manner: "*I ask why only the iris? Why not take photos from our bodies inside out, from the top to the bottom?*" (P6-III). Moreover, the fear of biometric data somehow being taken without one's consent was also mentioned: "*But if they take it, then you may not even know that they did*" (III).

With regards to surveillance technologies used for the tracking of people, while the use of GPS in mobiles was generally considered as acceptable, the electronic tagging of people through the use of RFID caused rather negative reactions amongst the respondents. The latter technology was perceived not only as impinging on privacy: "*It would feel very strange to know that somebody is stalking me all the time*" (P3-I) but also as limiting an individual's freedom of movement. It also provoked a comparison of humans being treated and dominated like 'objects': "*People are not animals*" (P12-I). Some participants again showed a rather sarcastic reaction to the notion of such extreme control: "*They would just need to add some microchip installed under the skin and everything would be fine. And then only to fix an antenna on our head to have a better signal [...]"* (III).

5.4 Surveillance Laws & Regulations

During the last part of the focus group sessions, the focus shifted to surveillance laws and regulations. A number of issues were discussed, including privacy rights, the effectiveness of surveillance laws and regulations, level of trust in the state and in private actors, length of data storage and issues of data sharing between different entities.

5.4.1 A lack of information and transparency

When discussing laws and regulations dealing with surveillance participants emphasised their limited knowledge and awareness with respect to privacy laws and, thus, about their rights as citizens: "*I know very little about the law"* (P11-I). Participants argued that laws lack transparency and moreover perceived the understanding of legislation as a difficult feat. In turn, this presented a difficulty for participants to determine whether the existing laws and regulations do indeed offer the required protection. It seems that participants were making assumptions about the content of the law according to their expectations.

5.4.2 Trust in the state and effectiveness of legislation

The second issue under discussion was the trust participants have in the Slovakian state. A number of participants expressed a rather scathing discontent and mistrust towards the state's protection of citizens' rights: "*What, in this state, would be respected*?" (P4-III) Not only did these participants argue that laws and regulations are not abided by, here possibly also alluding to a lack of enforcement, but they also appear to perceive the current legislation as inadequate: "*No, they [privacy rights] are not respected, and even if they were respected, we would probably not feel sufficiently protected"* (P7-II). To a large extent, participants not only expressed a high level of mistrust, but also a certain degree of helplessness in relation to the protection of their private data by the state, which they assumed to originate from historical experiences during socialism:

> "*In this state it does not happen how we would like to have it. The opposite is true. We have systems for the protection of personal data but they are not respected. Everything would be all right if they were respected, but it will take three to four generations to achieve this. We [our generation] will never reach such a state, it will remain for a long time the way it was during socialism*" *(III).*

A further critical issue influencing trust in the state was a perceived sense of injustice due to corrupt practices occurring in Slovakia. A number of participants here argued that certain 'powerful' citizens who have *"proper contacts"* (III) do not suffer any repercussions for crimes committed. The sense of injustice, and resignation, as a result of such a perception was evident amongst the respondents: *"[…] But the system works in such a way, that it is catching only the small fish but not the big ones*" (P5-III).

Two opposing views on the perceived general effectiveness of privacy laws were evident. Some participants were of the opinion that current legislation is both ineffective and untrustworthy: *"I think there are loopholes in laws and I do not feel protected by them. I don't have any suggestions which could make me feel safe, because I do not trust laws*" (P8-I). On the other hand, other participants were satisfied with and displayed trust in privacy laws despite acknowledging their lack of understanding of the legislation: "*Even if I do not know exactly what the law says, I believe that it is good*" (P3-I).

5.4.3 Length of data storage and accessibility

In general, the expectations of participants regarding the storage of their private data were largely similar throughout the focus groups in terms of a preference towards a limited and short length of data storage. The type of surveillance tool employed for the collection of data was deemed as important for most participants, since this was perceived as determining whether the type of data collected was of a personal, impersonal or sensitive nature. The type of data itself was therefore seen as a crucial factor for the determination of an acceptable storage period.

Generally, the more private the data was considered to be, the more issues of data storage became subject to debate. For instance participants argued that the storage of biometric data should not exceed a time span of between one week and one month. In contrast, the storage of number plate data was considered as more acceptable since, as some participants maintained, such type of information is less personal: "*Number plate recognition does not give much private information, as somebody else could drive my car*" (P1-I).

Moreover, the purpose of data storage, its use and its potential contribution to personal safety were considered as important aspects when considering length of storage. As a case in point, for the investigation of crimes, more tolerance was shown towards a longer storage time. On the other hand, some participants clearly disagreed with an indiscriminate storage of personal data pertaining to *all citizens*:

> "*Data should be collected only from criminals, [...] in which case it can be retained for even 10 years, but not from all other people, who did not commit a crime. [...] I do not agree with a general recording of the data of all citizens*" (P3-II).

In relation to this, a number of participants expressed their desire for a clear legal specification of data storage conditions: "*In the law it should be explicitly defined what information can be recorded and stored and for how long. Even the security of the data and access to them should be defined*" (P12-I).

5.4.4 Data sharing between different actors

The idea of data sharing between different parties made participants feel vulnerable due to the awareness of its possible misuse by a variety of entities. Therefore, the sharing of data in general was regarded negatively, although a difference in tolerance could be noticed regarding whether the sharing

occurred between public actors or private actors. In relation to this, data sharing between private entities was considered as possibly resulting in a higher risk of misuse, as opposed to when data was shared among public entities. On a general note, participants argued for an increase in measures aimed at preventing data misuse and additionally claimed that the sharing of data should require citizens' consent.

Specifically in relation to data sharing between private entities, it was evident that a number of participants were highly aware of such extensive data sharing, and some expressed their reservations, and discomfort, about this:

> "*How many times the phone is ringing and somebody is calling me directly with my name and offering some services that I was never seeking from anybody. And of course they know a lot of information about me and [I ask] from where?*" (III).

It appears that a very sensitive field for the participants was the sharing of health data by public institutions with private entities, because it gave participants the impression that moral values were gradually being lost, due to financial and business interests taking over and becoming an over-arching priority. Nevertheless, it appears that participants generally accepted the sharing of specific life-saving health data between public entities.

6. Conclusion

Slovakian participants showed a high awareness for surveillance and massively integrated dataveillance of citizens in the main spaces considered during the discussion. In general, participants perceived surveillance data as being collected for a number of purposes. Such purposes were usually contingent on the context; while for instance in boundary spaces and in common public spaces surveillance data was perceived as being employed mainly for security reasons, in commercial spaces surveillance data was considered as being primarily collected for marketing and business-related reasons.

With regards to the acceptance of technologically-mediated surveillance, it appears that different types of technologies meet varying levels of acceptance. The collection of data by traditional surveillance tools such as CCTV systems appeared to be widely accepted for security reasons and also considered as justified from a legal viewpoint. However, in spite of this, several participants regarded surveillance measures as rather inefficient in terms of the interests and protection of 'ordinary' citizens.

In general, it appears that participants' acceptance was contingent on a number of criteria; in particular, surveillance was considered as unacceptable in cases where data collected was overly personal in nature and when surveillance was covert. On the other hand, the use of biometric technologies and electronic tagging was perceived as particularly intrusive and unacceptable since such use was not only considered as a violation of privacy, but also as presenting a risk to citizens' freedom.

Overall, a number of participants expressed a lack of understanding in relation to the operational nature of smart technologies. Additionally, a sense of unease seemed to surround the automatic decision-making process of these technologies, which was perceived as possibly resulting in misinterpretation or in erroneous conclusions. On the other hand, less human involvement in the surveillance and judgement process seemed to reassure participants who consequently expected such an automatic process to result in a deceased risk of misuse, manipulation and corruption.

On a more general note, two prevalent concerns which emerged in relation to surveillance were the risk of misuse of personal data and the fear that extreme surveillance could result in the manipulation and control of citizens. With regards to risk of misuse, the collection of data specifically by private actors was linked to a high uncertainty regarding its use and further processing. Moreover, the collection of data by public actors raised fears of constant monitoring by the state. Such fears were especially prevalent amongst the older participants who experienced the socialist system in Slovakia and showed a low trust in the state and in existing protective mechanisms. A number of participants felt helpless in the face of surveillance and the loss of control over their personal data.

Although opinions varied in the different groups, doubts were raised in relation to whether surveillance measures actually provide a viable solution for the reduction or elimination of crime. Nevertheless, a number of participants were willing to sacrifice their privacy to a certain extent for the sake of increased safety in a context of escalating criminality.

A lack of knowledge and awareness was expressed regarding privacy legislation in Slovakia. Participants expressed a low level of trust into the state's protective mechanisms and there was a widespread criticism of corrupt practices, which ultimately contributed to a feeling of helplessness vis-à-vis citizens' ability to protect their privacy and personal data. In conclusion, the data appears to indicate that most participants perceived the threat that authorities could possibly take advantage of the power provided by the use of surveillance, thus leading to a situation where citizens' rights are compromised.

Acknowledgements

This research was carried out as part of SMART (Scalable Measures for Automated Recognition Technologies) a project that was funded by the European Union under the Seventh Framework Programme (2007-2013), Grant Agreement Number 261727.

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

- ☐ Metropolitan city
- ☐ Urban town
- ☐ Rural area

(A4) What is your highest level of education?

- ☐ Primary
- ☐ Secondary
- ☐ Post-secondary
- ☐ Upper secondary
- ☐ Tertiary
- ☐ Post graduate

(A5) What is your occupation?

- ☐ Managerial & professional
- ☐ Supervisory & technical
- ☐ Other white collar
- ☐ Semi-skilled worker
- ☐ Manual worker
- ☐ Student
- ☐ Currently seeking employment
- ☐ Houseperson
- ☐ Retired
- ☐ Long-term unemployed

Section B

(B1) Have you travelled by air during the past year (both domestic and international flights)?

- ☐ Yes
- ☐ No

(B2) Have you crossed a border checkpoint during the last year?

- ☐ Yes
- ☐ No

(B3) Have you ever been part of a large crowd (such as during a concert, rally or sports event)?

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

(B5) Which of these following devices do you make use of on a regular basis?

- ☐ Computer
- ☐ Laptop
- ☐ Tablets
- ☐ Mobile phone
- ☐ Smart phone
- ☐ Bluetooth
- ☐ In-built cameras (e.g. those in mobile devices)

(B6) If you make use of the internet, for which purposes do you use it?

- ☐ Social networking
- ☐ Online shopping
- ☐ File sharing
- ☐ To communicate (by e-mail etc.)
- ☐ To search for information
- ☐ To make use of e-services (e.g. internet banking)
- ☐ Other activities (please specify):

(B7) Have you made use of any e-government service (including services related to health care, tax purposes and welfare assistance) to make contact with any government agency during the past year?

- ☐ Yes
- ☐ No

(B8) Have you or are you currently receiving any benefits or grants (such as a stipend, scholarship, pension, unemployment benefits etc) from the government?

- ☐ **Yes**
- ☐ **No**

(B9) *Have you given your personal information to a commercial business (local and online) during the past year?*

- ☐ Yes
- ☐ No

(B10) Which of the following personal credentials do you make use of?

- ☐ Identity card
- ☐ Driving licence
- ☐ Passport
- ☐ Payment cards (e.g. credit, debit cards)
- ☐ Store / loyalty card

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

Introduction	Briefing
Welcome of participants - *Greeting participants* - *Provision of name tags* - *Signing of consent forms*	*Welcome the participants as soon as they come in. Assign them a seat and provide them with a name tag.* *Distribute the consent form to the participants and ask them to read and sign the form before the start of the focus group. This is important in order to ensure that the participants understand what they have agreed to do.*
Introduction [about 10 min] - *Thank you* - *Introduction of facilitating team* - *Purpose* - *Confidentiality* - *Duration* - *Ground rules for the group* - *Brief introduction of participants*	**Welcome to this focus group and thank you for agreeing to participate in this session. We appreciate that you took this time out of your busy schedule to participate in this project and your involvement is highly valued.** **My name is _____ and I will be facilitating the group discussion. I will be assisted by _____ my co-moderator, who will be taking notes and recording our discussion.** *Introduce any other colleagues who might also be present* **Our session will take between an hour and a half to two hours and since we will be tape recording the discussion, I would kindly ask you to speak in a clear voice; your opinions and thoughts are very important for this research, and we do not want to miss any of your comments.** **As previously mentioned when you were originally contacted to participate in this discussion, this focus group is on the topic of Technology and Privacy, and it is being conducted as part of the SMART Project, which is co-funded by the European Union. For those of you who wish to know more about the SMART Project, kindly let us know and we will proceed to give you more information at the conclusion of the focus group.** *At this stage it is important not to divulge any additional details on the content of the focus group in order to avoid influencing and biasing the ensuing discussion.* **As we already informed you when you read and signed the consent form, everything that will be recorded during this session will be kept confidential and your identity will remain anonymous. This means that your comments will be shared only by those involved in this study and used in scientific publications related to this study, and they will be anonymised before being reported. Hence, the information which will be included in the report will not in any way identify you as a**

	participant. In order to do this, each of you will be assigned a number, and it is this number that will be used in the report. **I also want to make sure that everyone in the group is comfortable enough to share their opinions. To make this possible, I would like to ask everyone present to follow these ground rules:** ▪ **We would like to hear from everyone in the group - we are interested in everyone's opinion** ▪ **There are no right or wrong answers so let us agree to respect each other's opinions** ▪ **Please make sure that your mobile phones are on silent so that the discussion will not get interrupted** ▪ **It is important that comments are made one at a time, since each participant's opinion is important. So let us agree to not speak at the same time, otherwise it will be difficult for us to capture everything that is said during the discussion** ▪ **Let's agree as a group to respect each other's confidentiality so that everyone feels more comfortable in speaking openly.** **If there is anyone who would like to suggest any other ground rules feel free to put your suggestions forward to the group.** **Does anyone have any questions before we start?** **Ok so let me start off by asking you to briefly introduce yourselves to the group without revealing private information. Let's do a round where you tell us your name and maybe something about you. I will start the round myself... *(carry out a brief personal introduction)*** *Running Total: 10 mi*
Objectives	**Discussion items and exercises**
Word association exercise **[About 5mins]** - *Word-association game serving as an ice-breaker* - *Establish top of mind associations with the key themes* - *Start off the group*	***Item 1*** **First up, we will carry out a short game: I will read out a word and I would like you to say the first couple of things that come to mind when you hear the word. Let's try an example first: What is the first thing that comes to mind if I say the word "*food*"? Preferably, try to think about single words or short phrases, avoiding lengthy descriptions.** *Read Out (one at a time):* *Technology, privacy, national security, personal information, personal*

discussion	*safety* ***Running Total: 15min***
Discussion on everyday experiences related to surveillance **[20min]** *- To explore participants' experience with surveillance & how they perceive it* *- To explore participants' awareness and knowledge of the different surveillance technologies*	***Item 2*** **Let's talk about something else. I want you to think about instances during which you feel that either you or your actions are being observed as well as any instances during which you are aware that information about you is being collected. Let's start by thinking about activities you would usually undertake in your everyday life. Let us take the following situations as examples of this.** **Scenario 1: Supermarket** ***As a first example we can take a shopping trip at your usual supermarket. Can you share your thoughts on this?*** **Scenario 2: Travelling** ***Let's move on to another situation, this time related to travelling. What about when you travel by air?*** **Scenario 3: Public place (e.g. museum, stadium)** ***Now imagine that you are visiting a public place, such as a museum or attending an event such as a sports match or a concert. What kind of activities do you think would be recorded?*** **Scenario 4: Mobile devices** **Let us discuss just one final example. Think about the times you use your mobile phone. What do you think is being recorded in this case?** *For each item, and where relevant, probe in detail to explore the following:* ***1. <u>How</u> is the information being collected:*** ***a. Which types of technologies do you think are used to collect your personal information?*** ***2. <u>What</u> type of information is being collected:*** ***a. What type of personal information do you think is being collected?***
Aims: *1. Explore the participants' awareness and knowledge of the technologies* *2. Explore the participants' experience of being monitored in their*	

many roles *3. Explore the participants' understanding of where their information is ending up* *4. Explore the participants' views on why their actions and behaviours are observed, monitored and collected*	***3. <u>Who</u> is collecting the information:*** ***a. Who do you think is responsible for collecting and recording your personal information?*** ***b. Where do you think your personal information will end up?*** ***4. <u>Why</u> the information is being recorded, collected and stored:*** ***a. Why do you think your personal information is being recorded and collected?*** ***b. In what ways do you think your personal information will be used?*** ***Running Total: 35min***
Presentation of cards depicting different technologies and applications [10mins] *To expose participants to a selection of relevant SMART technologies & applications in order to enable a better understanding and hence to facilitate the discussion.*	***Item 3*** *Present the following three cards (each depicting a group of different technologies and applications) to the group. The cards will include the following depictions:* ***Card 1 – Person or event recognition & tracking technologies**: Automated moving of closed circuit television (CCTV) cameras; Automatic number plate reader (ANPR) or automatic vehicle number identification (AVNI); and tracking devices such as mobile phone tracking and RFID* ***Card 2 - Biometrics**: Biometric technologies including fingerprint and iris scanning; and automatic facial recognition (AFR)* ***Card 3 - Object and product detection devices**: Knife arches (portal) and X-ray devices* ***Running total: 40min***
Presentation of MIMSI scenario to participants **[30mins]** - *To explore participants' understanding of*	***Item 4*** *Present the following hypothetical scenario to the group. A recording of the phone conversation can be prepared beforehand and presented to the group.* ***Phone conversation with the Customer Care Agent at the main branch of the Public Employment Service***

the implications of MIMSI

- *To explore participants' feelings, beliefs and attitudes vis-à-vis the sharing of personal information*

***Customer Care Agent**: Good morning this is Sharon speaking, how are you Mr. Brown? We were expecting your call after your work contract ended over a month ago.*

***Mr. Brown**: Erm...yes in fact that's why I'm calling...*

***Customer Care Agent**: Well, I'm actually not surprised you called now...how was your holiday in Cyprus? I am sure your wife and kids enjoyed the resort you were staying in...*

***Mr. Brown**: Yes it was a lovely holiday...and how do you know all this?*

***Customer Care Agent**: Well, it is in the system, Mr. Brown....obviously. Anyways, better get a head start on finding a new job...what with the cost of your family holiday and your car payment coming up soon...not to mention your VISA payment on the 22nd of this month...*

***Mr. Brown**: Is this also in your system?*

***Customer Care Agent**: Yes, of course Mr. Brown. By the way, good choice on the book you bought online...I read it myself and it gave me some really good tips...*

***Mr. Brown**: Hmmm...ok...regarding this new job seeker service, do I need to provide an updated photo of myself?*

***Customer Care Agent**: No Mr. Brown, that is already taken care of, of course! We have plenty of recent photos in our system. Which reminds me...lovely suntan you got on your holiday! Must have been beautiful weather! Before I forget, regarding the photo, do you prefer one with your glasses or one without?*

***Mr. Brown**: Oh...well....without is fine...so about my registration, can we set up an appointment for sometime next week?*

***Customer Care Agent**: Let me check our system...what about Wednesday at noon? Oh wait a second! I just noticed that you have a doctor's appointment scheduled right at that time. And I'm sure you don't want to miss that since monitoring your cholesterol level is surely important! How about Thursday first thing in the morning at 9am?*

***Mr. Brown**: Thursday morning will be fine...do I need to bring any documentation with me?*

***Customer Care Agent**: No Mr. Brown, we already have all the information we need in our system.*

***Mr. Brown**: I'm sure...*

***Customer Care Agent**: Thank you for calling Mr. Brown and we will see you next week. By the way, enjoy your cappuccino at Cafe Ole'...*

***Mr. Brown**: I am...goodbye...*

Aims

After presenting the previous scenario to the group, probe in-depth to explore the following:

1. Participants' first reactions including:

Possibility / impossibility of scenario

1a. How would you feel if this happened to you?
(Also probe to establish the degree of control / helplessness felt by the participants in such a hypothetical scenario)

1b. How would you react if this happened to you? What would you do?

Acceptability / unacceptability of scenario

1c. Is such a scenario <u>possible / impossible</u>?

1d. Is such a scenario <u>acceptable / unacceptable</u>?

2. Participants' beliefs and attitudes on how technology affects or might affect their privacy

2a. To what extent do you think that "<u>stand alone</u>" (individual technologies) affect your privacy?

2b. To what extent do you think that "<u>smart technologies</u>" i.e. those which process data in an <u>automatic</u> (or semi-automatic) manner affect your privacy?

3. Participants' beliefs and attitudes in terms of the type of information such as: Medical & financial data; photos and location.

3a. What type of personal information do you find <u>acceptable</u> to being collected, used and / or shared?

3b. What type of personal information would you <u>object</u> to being collected, used and / or shared?

4. Participants' beliefs and attitudes on the collection, usage and sharing of personal information with third parties.

4a. What do you think about having your personal information collected, used and shared by the <u>state</u>?

4b. What do you think about having your personal information collected, used and shared by <u>private entities</u> (such as commercial ones)?

5. Participants' beliefs and attitudes on the benefits and drawbacks of being monitored

5a. Do you think there are any <u>benefits</u> to having your actions and behaviour monitored?

5b. Do you think there are any <u>drawbacks</u> to having your actions and behaviour monitored?

Running Total: 1 hour 15min

Reactions to scenarios

[About 20mins]

- *To stimulate a debate in order to explore the participants' perceptions of the "security vs. privacy trade-off".*
- *Here, the discussion should not focus on whether these technologies will increase security - this should be taken as a given. The discussion should mainly centre on whether these technologies effect privacy and hence revolve around the security - privacy trade-off*

Item 5

During the next exercise, we will be discussing the following hypothetical scenario. Imagine the following scenario:

Due to an significant increase in <u>*violent crimes*</u> in the capital city, including <u>*a spate of kidnappings and murders which seem random and unconnected*</u>, the state has decided to introduce CCTV surveillance in every public space, both those publicly owned (such as subways, public gardens and public conveniences) as well as those privately owned (such as shops, malls and taxis) which will enable automated face-recognition. In addition, all the cars passing through the main check points will have their number plates recorded. There are also plans to install sensors in all public areas which are able to detect loud noises such as in the case of someone screaming. All citizens will be required to have their DNA and fingerprints collected, and their iris scanned. The state has also decided that all citizens who are identified as presenting a possible risk to others should be electronically tagged to monitor and track their movements. For their safety, elderly people and children up to the age of 12 years will also be electronically tagged. All the data from these different technologies will be stored in linked databases administered by the police, who will be notified automatically should there be a cause for alarm and risk to any citizen.

Tell the participants to imagine the above scenario however with the following variations:

Variation 1: Even though a significant increase in violent crime is taking place throughout the majority of neighbouring cities, the city you reside in is not experiencing any increase in crime. However the state still decides to introduce the surveillance measures as a precaution.

Variation 2: The entire country has a very low crime rate in general, but the state still decides to introduce the surveillance measures as a precaution after a neighbouring city experienced an isolated incident during which a number of people were gunned down and seriously injured by a man who opened fire in a shopping mall.

Aims:

1. Security climate and level of threat

2. Deployment of specific technologies

3. Locations of deployment such as:
Airports
Malls
Streets

4. Existence of laws and other safeguards (in relation to the collection, storage and use of data)

During the discussion of the above scenario/variations, probe in detail to explore the following factors and how they might affect the "security vs. privacy trade off":

1a. What makes you feel <u>safe</u> in the scenario provided?

1b. What makes you feel <u>vulnerable</u> in the scenario provided?

1c. Would you be willing to sacrifice your privacy if the level of threat was different as in variation 1 and 2 of the scenario?

2. From the smart technologies depicted in the scenario, i.e.
CCTV with Automated Facial Recognition,
Automatic Number Plate Recognition (ANPR),
Sensors (with the ability to detect loud noises),
Biometric technologies (including fingerprinting) and
Electronic tagging (which uses RFID)

2a. Which technologies do you consider <u>acceptable</u>? Why?

2b. Which technologies do you consider <u>invasive</u> and as a threat to your privacy? Why?

2c. What do you think of these automated (or semi-automated) technolgies whereby the final decision is taken by the system and not by a human operator?

3a. Which locations do you consider <u>acceptable</u> in relation to being monitored? Why?

3b. Which locations do you consider <u>unacceptable</u> in relation to being monitored?

4a. What do you think about privacy laws? Do they make you feel <u>protected</u>?

4b. Are there any <u>safeguards</u> or conditions that you would find

	reassuring?
5. Length of storage of surveillance data	***5a. What do you think about the length of storage of surveillance data? Does it make a difference?*** ***To help you probe, provide the following examples to the participants:*** - ***Recordings of CCTV*** - ***The location and movement of cars*** - ***The storage of DNA, fingerprints and iris scans*** - ***The location of citizens who pose a risk to others*** - ***The location and movements of elderly people and children*** ***5b. If length of storage makes a difference, what would you consider as an acceptable timeframe?*** ***Running Total: 1 hour 35min***
Brief summary of discussion [5mins] ▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***Item 6 – Summing up session*** ***At the end of the focus group, it is helpful to provide a summary of the emerging points. Here you should aim at giving a brief summing up of the themes and issues raised during the discussion. After, you can ask for the following from the participants:*** - ***"How well does that capture what was said here today?"*** - ***"Is there anything we have missed?"*** - ***"Did we cover everything?"*** - ***This brief session will give participants an additional opportunity to express their views and can also be used to elaborate on topics raised but not pursued at the time.*** ***Running Total: 1 hour 40 min***
Conclusion of focus group [5mins] ▪ ***Thank the participants*** ▪ ***Hand out the reimbursement***	***Item 7 –Closure*** **With this last exercise our discussion has come to an end. May we take this opportunity to once again thank you for joining us and for sharing your opinions, experiences and thoughts.** ***At this point, hand out the reimbursements to the participants and inform the participants about the next steps.***

▪ ***Give information on SMART***	***Give out more information about the SMART to the participants requesting such information.*** ***Total: 1 hour and 45 min***

APPENDIX C – DISCUSSION GUIDELINES (SLOVAK)

Introduction	Briefing
Privítať účastníkov -	*Privítajte účastníkov hneď ako vstúpia do miestnosti. Posaďte ich a dajte im menovky.* *Rozdajte formulár, v ktorom súhlasia s účasťou a požiadajte ich, aby si ho prečitali a podpísali skôr ako sa začne skupinova diskusia. Toto je dôležité kvôli tomu, aby účastníci rozumeli tomu, čo budu robit.*
Introduction [10 mins]	**Vitajte v tejto focus skupine a ďakujeme Vám, že ste súhlasili zúčastniť sa na tomto projekte. Vážime si, že ste si našli čas aj keď určite ste sami veľmi zaneprázdnení. Váš prínos pre tento projekt je veľmi oceňovaný.** **Volám sa _____ a budem koordinátorom tejto skupinovej diskusie. Pomáhať mi bude _____, môj spolu koordinátor jeho/jej úlohou bude robiť si poznámky a nahrávať celú diskusiu.** *Predstavte všetkých ďalších členov týmu, ktorí by sa mohli zúčastniť.* **Naša diskusia bude trvať niečo medzi hodinkou a pol a dvoma hodinami a pretože táto diskusia bude nahrávaná tak Vás chceme poprosiť, aby ste hovorili dostatočne hlasne a zrozumiteľne, pretože každé Vaše slovo je pre tento projekt veľmi dôležité.** **Ako bolo už predtým spomenuté keď sme Vás povodne kontaktovali, témou tejto diskusnej skupiny je Technológie a Súkromie a je súčasťou SMART projektu. Pokiaľ chcete viac informácií o SMART projekte, dajte nám vedieť a my Vám poskytneme všetky informácie na konci tejto skupinovej diskusie.** *V tejto fáze je dôležité aby nedošlo k prezradeniu žiadnych ďalších podrobností o obsahu diskusie, aby účastníci neboli ovplyvnený a tým ani nebola ovplyvnená celá diskusia.* **Ako sme Vás už informovali keď ste čítali a podpísali Váš súhlas s účasťou, všetko čo sa bude nahrávať bude považované za dôverné a Vaša identita bude anonymná. To znamená že komentáre z tejto diskusie budú spracovávané iba za účelmi tejto štúdie a predtým budú anonymizované. Preto informácie, ktoré získame touto diskusiou nebude možné nijakým spôsobom spojiť s Vašou osobou. Za týmto účelom každému z Vás bude priradené číslo, ktoré bude použité v reporte z tejto diskusie.** **Tiež je veľmi dôležité aby sa každý v tejto skupine cítil dostatočne pohodlne k tomu aby sa podelil o svoje názory. Kvôli splneniu tohto cieľa Vás chceme požiadať aby ste sa riadili nasledujúcimi pravidlami:** ▪ **Chceli by sme počuť názor každého zo skupiny. Máme záujem o každého názor.** ▪ **neexistujú správne a nesprávne odpovede. Rešpektujeme každý názor.** ▪ **Prosím Vás uistite sa že Vaše telefónny sú stíšené, aby nedošlo k prerušeniu diskusie.** ▪ **Je veľmi dôležité neskákať druhým do reči. Každý názor je pre nás dôležitý a keby rozprávali viacerí ľudia naraz, bolo pri pre nás nemožné interpretovať názor každého z Vás.** ▪ **Ako celok sa dohodnime na rešpektovaní anonymity ostatných, aby každý odpovedal voľne.**

	Ak máte návrhy na nejaké iné pravidlá, prosím poskytnite nám Vaše návrhy. **Ma niekto ešte nejaké otázky predtým ako začnime?** **Dobre, začnime teda tým, že sa každý predstaví. predstavujte sa prosím bez toho aby ste poskytli o sebe dôverné informácie. Skúste nám povedať Vaše krstné meno a možno niečo o sebe. Ja začnem... *(pokračuje predstavovanie)*** *Running Total: 10 min*
Objectives	**Discussion items and exercises**
Word association exercise **[5 mins]**	***Bod 1*** **Najprv si zahráme krátku hru. Prečítam Vám slovo a od Vás by som chcel aby ste mi povedali prvých pár slov čo Vás ako prvé napadnú. Napríklad pri slove Potrava?. Preferované sú jednoslovné odpovede a krátke frázy a vyvarujte sa dlhých viet** *Postupne čítaj: Technológia, súkromie, národná bezpečnosť, osobná informácia, osobná bezpečnosť* *Celkové trvanie:15 min*
Discussion on everyday experiences related to surveillance **[20 mins]**	***Bod 2*** **Poďme hovoriť o niečom inom. Uvažujte o prípadoch, počas ktorých máte pocit, že buď vy alebo vaše akcie sú pozorované, rovnako ako všetky prípady počas ktorých ste si vedomí, že informácie o vás sa zhromažďujú. Začnime tým, že budete premýšľať o aktivitách, ktoré obvykle vykonávate vo svojom každodennom živote. Zoberme si nasledujúce situácie ako príklad.** **Scenár 1: Supermarket: Ako prvý príklad si môžeme vziať nákupy v Vašom bežnom supermarkete. Môžete sa podeliť o Vaše úvahy v tomto smere?** **Scenár 2: Cestovanie: Poďme na inú situáciu, tentoraz v súvislosti s cestovaním. Napríklad pri ceste lietadlom?** **Scenár 3: Verejné miesto (napr. múzeum, štadión): Teraz si predstavte, že ste navštívili múzeum, športový štadión, koncert alebo iné verejné podujatie. Aké činnosti by mohli byť zaznamenávané?** **Scenár 4: Mobilné zariadenia: Diskutujme ešte jeden posledný príklad. Myslite o situácii keď používate Váš mobilný telefón. Čo si myslíte že by mohlo byť zaznamenávané pri používaní mobilného zariadenia?** *Pre každý scenár preskúmajte nasledujúce veci(ak je to relevantné):* ***1. Ako sú informácie zbierané:*** ***a. Aké technológie sú využívané pri zbieraní Vašich osobných informácií?*** ***2. Aké typy informácií sa zbierajú:*** ***a. Aké typy osobných informácií sa zbierajú?***

3. Kto zbiera informácie:

a. Kto podľa Vás je zodpovedný za zbieranie a nahrávanie vašich osobných informácií?

b. Kde, podľa Vás, skončia Vaše osobné údaje?

4. ***Prečo sú informácie zbierané a nahrávané a uchovávané:***

a. Prečo si myslite že sú Vaše osobné informácie nahrávané a zbierané?

b. Akým spôsobom budú Vaše osobné údaje využívané?

Celkové trvanie:35min

Presentation of cards depicting different technologies and applications [10 mins]

Bod 3

Odprezentujte nasledujúce tri karty skupine(každá zobrazuje inú skupinu rôznych technológií). Karty obsahujú nasledujúce skupiny technológií:

***Karta1 – Person or event recognition & tracking technologies**: Automatické presúvanie uzavretého televízneho okruhu kamery (CCTV); Automatický identifikátor evidenčných čísiel vozidiel. a sledovacie zariadenie na sledovanie mobilného telefónu a RFID.*

***Karta 2 - Biometrické**: Biometrické technológie zahŕňajúce snímanie odtlačkov prstov a sietnic a technológia na automatické rozoznávanie tváre (AFR)*

***Karta 3 – Technológie na detekciu objektov**: Detekcia kovu a röntgenová detekcia.*

Celkové trvaniel: 40min

Presentation of MIMSI scenario to participants [30 mins]

Bod 4

Prezentujte nasledujúci hypotetický scenár skupine. Záznam telefónneho hovoru môže byť pripravený vopred.

Telefonický rozhovor s pracovníkom úradu práce.

Pracovník: *Dobrý deň volám sa Sharon, ako sa máte Pán Brown? Čakali sme, Váš hovor keďže Vaša zmluva skončila už pred mesiacom.*
Pán Brown: *Ehm ... áno to je dôvod, prečo volám* ***...***
Pracovník: *No, ja vlastne ani nie som prekvapená, že ste zavolali práve teraz ... aká bola vaša dovolenka na Cypre? Som si istá, že vaša manželka a deti si ju určite užili. Vybrali ste si naozaj nádhernú destináciu.*
Pán Brown: *Áno, bola to krásna dovolenka ... a ako o tom všetkom viete?*
Pracovník: *No, mám to samozrejme v systéme, Pán Brown ....Tak ako tak, je dobré že si hľadáte prácu v predstihu... čo s nákladmi na rodinnú dovolenku a splátku Vášho nového auta už tiež čoskoro musíte zaplatiť... nehovoriac o inkasách, ktoré majú odísť z Vášho účtu 22. tohto mesiaca...*
Pán Brown: *Aj to máte v systéme?*
Pracovník: *Áno, samozrejme, pán Brown. Mimochodom, dobrá voľba knihy, ktorú ste zakúpili on-line ... Čítala som to a to a je to naozaj kvalitné čítanie…*
Pán Brown: *Hmmm ... ok ... pokiaľ ide o túto novú službu uchádzačov o zamestnanie, musím poskytnúť svoju aktuálnu fotku?*
Pracovník: *Nie nie pán Brown, o to je už samozrejme postarané! Máme veľa Vašich aktuálnych fotografií v našom systéme. Čo mi pripomína ... krásne opálenie z dovolenky! Museli ste mať naozaj krásne počasie! Než by som bola zabudla, pokiaľ ide o fotografiu, dávate prednosť s okuliarmi, alebo bez?*
Pán Brown: *Oh ... dobre .... bez je v poriadku ... tak o mojej registrácii, môžeme sa dohodnúť na schôdzke niekedy budúci týždeň?*
Pracovník: *Pozriem sa do nášho systému ... čo tak stredu napoludnie? Ale počkajte sekundu! Len som si všimol, že máte termín u lekára plánovanú práve v tejto dobe. Som si istý, že Vaša hladina cholesterolu je isto veľmi dôležitá. Čo tak vo štvrtok ráno o 9:00?*
Pán Brown: *Štvrtok ráno bude v poriadku ... mám priniesť nejaké dokumenty so sebou?*
Pracovník: *Nie pán Brown, už máme všetky informácie, ktoré potrebujeme v našom systéme.*
Pán Brown: *Som o tom presvedčený ...*
Pracovník: *Ďakujem za zavolanie pán Brown a uvidíme sa budúci týždeň. Mimochodom, užite si cappuccino v Cafe Ole "...*
Pán Brown: *Ehm ... zbohom ……*

Po odprezentovaní predošlej scénky do hĺbky preskúmajte nasledujúce:

1a. Ako by ste sa cítili keby sa to stalo práve Vám?

(Tiež otestujte mieru kontroly/bezradnosti, akú by pociťovali)

1b. Ako by ste reagovali keby sa to stalo práve Vám? Čo by ste

robili?

1c. Je takýto scenár podľa Vás možný/nemožný?

1d. Je takýto scenár akceptovateľný/neakceptovateľný?

2a. Do akej miery ovplyvňujú tkz. „stand alone“ technológie Vaše súkromie?

2b. Do akej miery ovplyvňujú SMART technológie(technológie, ktoré spracovávajú dáta automatizovane/poloautomatizovane) Vaše súkromie?

3a. Pre ktoré osobné informácie je prijateľné aby boli zbierané, , využívané alebo posúvané ďalej?

3b. Ktoré osobné informácie považujete naopak za neprijateľné aby sa zhromažďovali, využívali alebo posúvali ďalej?

4a. Čo si myslíte o tom keby vaše osobné informácie zbierala, zhromažďovala a využívala vláda a štátne organizácie?

4b. Čo si myslíte o tom keby vaše osobné informácie zbierala súkromná spoločnosť(napr. pre komerčné využitie)?

5a. Myslíte si že by ste mohli mať nejaké výhody z toho že je Vaše správanie sledované?

5b. Naopak, existujú podľa Vás nevýhody takéhoto konania?

Celkový čas 1 hodina 15min

Reactions to scenarios

[About 20mins]

Bod5

V nasledujúcej úlohe budeme diskutovať nasledujúci hypotetický scenár. Predstavte si nasledujúci scenár:

Kvôli výraznému nárastu násilných trestných činov v hlavnom meste, vrátane únosov a vrážd, ktoré nemajú spolu zdanlivo žiadnu súvislosť, vláda sa rozhodla zaviesť kamerový systém s automatickým rozoznávaním tvárí na každé verejné (ako napríklad metro, verejné záhrady alebo záchody) ale aj súkromné (ako napr.: Obchodné centrá a taxíky) priestranstvá. Okrem toho budú všetky hlavné dopravné uzly monitorované kamerami, ktoré budú obsahovať systém na rozoznávanie evidenčných čísiel vozidiel. Tiež vláda plánuje zaviesť na všetky verejné priestranstvá systém na rozoznávanie hlasných zvukov. Úlohou tohto systému bude zaznamenávať napríklad výkriky alebo hlasné volania o pomoc. Všetkým občanom bude tiež odobratá DNA, odtlačky prstov a ich sietnice budú naskenované. Vláda sa tiež rozhodla, že všetky osoby, ktoré predstavujú potencionálne riziko budú vybavené elektronickým zariadením na sledovanie ich pohybu. Pre ich bezpečie budú tiež takto monitorovaný dôchodcovia a deti pod 12 rokov. Všetky dáta získané týmito technológiami budú uložené v policajných databázach a budú spracované automaticky a v prípade nebezpečenstva vyšlú alarm kompetentným osobám.

Povedzte účastníkom nech si predstavia scenár v nasledujúcich variantoch:

Variant 1: Vo všetkých veľkých susedných mestách je nárast kriminality ale práve vo Vašom meste tento nárast nie je napriek tomu sa vláda rozhodne zaviesť tieto opatrenia aj vo Vašom meste ako preventívne opatrenie.

Variant 2: Celková kriminalita v krajine je nízka, ale nastal ojedinelý incident v susednom mesto, pri ktorom zahynulo alebo sa zranilo niekoľko ľudí pri úmyselnom podpálení nákupného centra.

Počas diskusie o vyššie uvedenom scenári / variante, detailne preskúmajte nasledujúce faktory a ako by mohli mať vplyv na kompromis medzi bezpečnosťou a súkromím

1a. Čo vám dáva pocit bezpečia keby nastal tento hypotetický scenár?

1b. Mali by ste naopak pocit zraniteľnosti? Prečo?

1c. Boli by ste ochotný obetovať svoje súkromie pri tomto scenári? Ako by sa zmenil Váš názor keby nastala varianta 1/ varianta 2?

2. Zo všetkých technológií spomenutých v týchto scenároch.

CCTV a Automatické rozoznávanie tvárí,
Automatické rozpoznávanie evidenčných značiek vozidiel (ANPR),
Senzory hlasného zvuku,
Biometrické technológie (vrátane odtlačkov)
Elektronické značkovanie (ktoré využíva RFID)

2a. Ktoré z týchto technológií sú pre Vás akceptovateľné a prečo?

2b. Ktoré z týchto technológií považujete za invazívne do Vášho súkromia a prečo?

2c. Čo si myslíte o týchto automatizovaných (alebo semi-automatizovanych) technológiách pri ktorých konečné rozhodnutie robí počítač a nie človek?

3a. Ktoré lokality sú pre Vás akceptovateľné na pozorovanie? Prečo?

3b. Ktoré lokality sú pre Vás neakceptovateľné na pozorovanie? Prečo?

4a. Čo si myslíte o zákonoch na ochranu súkromia? Cítite sa byt chránený?

4b. Existujú nejaké záruky alebo podmienky, ktoré by Vás upokojovali?

5a. Čo si myslíte o dĺžke uchovávania dát o sledovaní. Myslíte, že je v tom nejaký rozdiel?

Pre pomoc poskytnite účastníkom nasledujúce možnosti:

Automatické rozoznávanie tvárí pomocou CCTV,
Automatické rozpoznávanie evidenčných značiek vozidiel (ANPR),
Uchovávanie DNE, odtlačkov prstov a iris zobrazení
Lokalizácia osôb ktoré sú rizikové pre iných
Lokalizácia a pohyby starších ľudí a deti

5b. Ak dĺžka ukladania dát hrá rolu, aká by bola pre Vás akceptovateľná?

Celkový čas: 1 hodina 35min

Cieľe	Zhrnutie diskusie
Zhrnutie diskusie **[5mins]**	***Bod 6*** ***Na konci diskusnej skupiny je vždy dôležité zhrnúť všetko to čo diskutujúci povedali. Tu by ste mali zosumarizovať stručne témy a problémy ktoré sa stali predmetom diskusie Poproste účastníkov o zodpovedaní nasledujúcich otázok:*** - **“Ako dobre vystihlo túto tému to čo tu bolo povedané?”** - **“Niečo sme opomenuli?”** - **“Pokryli sme všetko?”** ***Toto zhrnutie umožní účastníkom vyjadriť svoje koncové názory a môže byť tiež nápomocné k rozpracovaniu tém ktoré sa vyskytli ale neboli***

	dostatočne prediskutovane v priebehu diskusie. ***Celkový čas: 1 hodina 40min***

Cieľe	Záver
Uzavrieť skupinu **[5mins]** ▪ ***Poďakovať účastníkom*** ▪ ***Poskytnúť ďalšie informácie***	***Bod 7*** **Týmto sme sa dostali na zaver nasej diskusie. Na záver by som Vám ešte raz chcel poďakovať za účasť a za to, že ste zdieľali s bani Vaše názory, skúsenosti a názory.** ***V tomto bode dajte účastníkom odmenu a informujte účastníkov o ďalších krokoch projektu.*** ***Taktiež poskytnite ďalšie informácie o SMART projekte tým účastníkom ktorí žiadali o také informácie.*** ***Celkový čas: 1 hodina 45 min***

APPENDIX D – DEBRIEFING FORM

SMART WP10 Focus Group De-briefing form	
1. Date	
2. Duration	
3. Facilitating team	Moderator: Co-moderator: Other team members:
4. Group composition 4a. Number of participants 4b. Gender ratio 4c. Age categories	 Participants present: Participant no-shows: Males: Females: 18-24 years: 25-44 years: 45+ years:
5. Overall observations 5a. **Group dynamics:** How would you describe the group dynamics / atmosphere during the session? 5b. **Discussion**: How would you describe the overall flow of the discussion? 5c. **Participants**: Were there any individual participants who stood out? (For instance, participants who might have been particularly talkative, dominant, silent or aggressive)	
6. Content of the discussion 6a. **Themes:** What were some of the most prominent themes and ideas discussed about? Did anything surprising or unexpected emerge (such as new themes and ideas)? 6b. **Missing information:** Specify any content which you feel was overlooked or not	

explored in detail? (E.g. due to lack of time etc.) 6c. **Trouble spots**: Were there any particular questions and/or items which did not lead to the desired information (kindly pinpoint which ones, if any)	
7. Problems or difficulties encountered Did you encounter any difficulties in relation to the following? If yes, kindly explain in detail. 7a. **Organisation and logistics** (For instance those relating to location, venue, any interruptions, reimbursement and refreshments) 7b. **Time management**: Timing of particular items in the discussion guidelines and timing of the overall discussion 7c. **Group facilitation** (For instance whether it was difficult to get the discussion going etc.) 7d. **Focus group tools** (For instance the recording equipment and handouts)	
8. Additional comments	

APPENDIX E – CONSENT FORM

You have been asked to participate in a focus group being conducted as part of the SMART Project, which is co-funded by the European Union. This focus group is being carried out by the *<insert name of institution here>* which is the co-ordinator for the SMART project in *<insert country here>.* The information obtained during this discussion plays a very important part in the research being carried out as part of this international project.

Participation

The focus group discussion will take approximately two hours. Your participation in this group is entirely voluntary and you may stop your participation at any time. You may also refuse to answer any questions with which you are uncomfortable. You may also withdraw your participation from the focus group at any time, and no penalties will be incurred should you withdraw from the study.

Confidentiality and anonymity

The discussion will be recorded however all personal information collected and your responses will be anonymised as soon as reasonably possible. Your name will not be connected to your responses; instead, a number will be utilised for identification purposes. In addition, any information which could potentially make it possible for you to be identified will not be included in any report. Your personal data will be kept confidential and it will only be disclosed to those individuals working on the SMART project on a need-to-know basis and it will not be disclosed to any other individual or third parties unrelated to the SMART project. Your anonymised comments might be used in scientific publications related to this study

Out of respect for each other, we kindly ask that the participants' responses be kept confidential. Nonetheless, we cannot offer any assurance that the participants will keep confidentiality.

Data protection and data security

All personal data collected will be kept secure and no personal data will be kept for longer than necessary for the purposes for which it was collected. Personal data which is no longer required for the purposes of the SMART project will be deleted.

Risks and benefits

No risks are foreseen to the focus group participants. Your participation in this research will most likely not result in any benefit to yourself; however it will assist the researchers concerned in providing valuable information on the topic under study.

Questions about the research

If you wish further information on the SMART Project, you can be given this information when the focus group discussion is concluded.

I confirm that I have read and understood the above information and I agree, out of my own free will and volition, to participate under the stated conditions.

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

- 1.1. Commercial space
  - 1.1.1. Awareness of different surveillance methods/technologies
    - 1.1.1.1. Financial monitoring
    - 1.1.1.2. Loyalty cards
    - 1.1.1.3. CCTV
  - 1.1.2. Perceived purposes
    - 1.1.2.1. Creation of customer databases
    - 1.1.2.2. Marketing and advertisement
    - 1.1.2.3. Theft prevention

- 1.2. Boundary space
  - 1.2.1. Awareness of different surveillance methods/technologies
    - 1.2.1.1. CCTV
    - 1.2.1.2. Monitoring of personal data
      - 1.2.1.2.1. Passport control
      - 1.2.1.2.2. Criminals record check
      - 1.2.1.2.3. Financial monitoring
    - 1.2.1.3. Object and product detection devices
      - 1.2.1.3.1. X-rays
      - 1.2.1.3.2. Body scanners
  - 1.2.2. Perceived purposes
    - 1.2.2.1. National security
    - 1.2.2.2. Organisational reasons
    - 1.2.2.3. General security
    - 1.2.2.4. Improvement of customer service
    - 1.2.2.5. Creation of databases and statistics
    - 1.2.2.6. Marketing

- 1.3. Common public spaces
  - 1.3.1. Awareness of different surveillance methods/technologies
    - 1.3.1.1. CCTV
    - 1.3.1.2. Electronic entry gates
    - 1.3.1.3. Monitoring of personal data
      - 1.3.1.3.1. Collection of personal data
  - 1.3.2. Perceived purposes
    - 1.3.2.1. Security
    - 1.3.2.2. Prevention of crime and crime investigation
    - 1.3.2.3. Creation of databases

1.3.2.4. Marketing and advertisement
1.3.2.5. Improvement of operations and customer service

1.4. Mobile devices and virtual spaces
1.4.1. Awareness of different surveillance methods/technologies
1.4.1.1. Monitoring of call lists and text messages
1.4.1.2. Monitoring of website logs
1.4.1.3. Location tracking via GPS
1.4.1.4. Recording of conversations (wiretapping)
1.4.2. Perceived purposes
1.4.2.1. Criminal investigations
1.4.2.2. Security
1.4.2.3. Marketing and sales

2. Perceptions and attitudes towards smart surveillance and integrated dataveillance
2.1. Feelings
2.1.1. Extreme discomfort
2.1.1.1. Fear
2.1.2. Helplessness and resignation
2.1.2.1. Power imbalance
2.1.2.2. Loss of control
2.1.3. Indignation and anger
2.1.3.1. Threat to privacy
2.1.3.2. Risk of misuse
2.1.4. Convenience
2.1.4.1. Efficient service
2.1.4.2. Personalised offers

2.2. Behavioural intentions
2.2.1. Passive reactions
2.2.1.1. Inertia
2.2.1.2. Resignation
2.2.1.3. Escape
2.2.1.4. Disconnection
2.2.2. Active reactions
2.2.2.1.1. Self-censoring
2.2.2.1.2. Take independent action
2.2.3. Take legal action
2.2.3.1. Investigate the legitimacy
2.2.3.2. Group with other citizens and complain

2.3. Beliefs
2.3.1. Likelihood of smart surveillance and integrated dataveillance
2.3.1.1. Technical aspect
2.3.1.1.1. Capacities of integration of data
2.3.1.2. Ethical aspect
2.3.1.2.1. General refusal of surveillance
2.3.1.2.2. Invasion of privacy
2.3.2. Perceived effectiveness of smart technologies and dataveillance
2.3.2.1. Decision-making capabilities of automated systems
2.3.2.1.1. Possible errors and misunderstandings
2.3.2.1.2. Wrong conclusions
2.3.2.2. Human factor
2.3.2.3. Programming for the recognition of behavioural patterns
2.3.2.3.1. Creation of individual records
2.3.2.4. Convenience
2.3.2.4.1. More respect of privacy: objectivity
2.3.2.4.2. Lower risk of data misuse

3. Security-privacy trade-offs
3.1. Acceptance of technological surveillance
3.1.1. Feelings
3.1.1.1. Vulnerability: surveillance produces insecurity
3.1.1.2. Crossing of borders and violation of rights
3.1.2. General beliefs
3.1.2.1. Fear of unjustified monitoring of citizens
3.1.2.2. Threat of data misuse and theft
3.1.2.3. Danger to freedom: possible manipulation and control
3.1.2.4. Violation of privacy and freedom
3.1.3. Effectiveness of surveillance
3.1.3.1. Ineffectiveness for crime prevention and investigation of crimes
3.1.3.2. Deterrent effect
3.1.3.3. Tracking of missing people
3.1.3.4. Increase of safety
3.2. Locations of deployment
3.2.1. Acceptable in public places and high risk areas: The ‘caring’ function of surveillance.
3.2.2. Unacceptable in private spaces and private spheres
3.3. Perceptions of different technologies
3.3.1. CCTV
3.3.1.1. Effect of normalisation
3.3.1.2. Mistrust and scepticism: no protection for customers
3.3.2. Sound sensors

3.3.2.1. Acceptance
3.3.2.2. Possibility of wrong conclusions
3.3.3. Biometric data
3.3.3.1. Vulnerability and uneasiness
3.3.3.2. Loss of control
3.3.3.3. Possibility of taking one's data without consent
3.3.4. Electronic tagging (RFID) and GPS
3.3.4.1. Impingement of privacy
3.3.4.2. Limitation of freedom of movement
3.3.4.3. Objectification of humans: extreme control

4. Surveillance laws and regulations

4.1. Feelings and beliefs
4.1.1. A lack of information and transparency
4.1.2. Trust in the state and effectiveness of legislation
4.1.3. Length of data storage and accessibility
4.1.4. Data sharing between different actors