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

Noellie Brockdorff[1], Christine Garzia[1], Simon Dobrišek[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Laboratory of Artificial Perception, Systems and Cybernetics, University of Ljubljana, Ljubljana, Slovenia

April 2014

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/

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 6
   - 3.3 Focus group procedure 7
   - 3.4 Data analysis 7
4. Description of the sample 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 13
   - 5.2 Perceptions & attitudes towards smart surveillance and integrated dataveillance 14
     - 5.2.1 Feelings 14
     - 5.2.2 Behavourial intentions 14
     - 5.2.3 Beliefs 14
       - 5.2.3.1 Likelihood of smart surveillance and massively integrated dataveillance 14
       - 5.2.3.2 Acceptance of smart surveillance and massively integrated dataveillance 15
       - 5.2.3.3 Perceived privacy impact and effectiveness of smart technologies 17
   - 5.3 Security-Privacy Trade-Offs 18
     - 5.3.1 Acceptance of technological surveillance 18
     - 5.3.2 Perception of different technologies 20
   - 5.4 Surveillance Laws and Regulations 22
     - 5.4.1 A lack of information or nonchalance? 22
     - 5.4.2 Effectiveness of the legislation 22
     - 5.4.3 Suggested safeguards 22
     - 5.4.4 Length of data storage 23
6. Conclusion 24

Acknowledgements 26

Appendices

A. Recruitment questionnaire 27
B. Interview guidelines (English) 28
C. Interview guidelines (Slovenian) 37
D. Debriefing form 47
E. Consent form 49
F. Coding map 51

1. Key Findings

This document presents the Slovenia 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 3 focus group discussions comprising of 28 participants from different age groups, which were held in order to examine the awareness, understanding, beliefs and attitudes of citizens towards smart surveillance and privacy.

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

The Slovenian participants were highly aware of being under surveillance in different contexts including commercial, boundary and public spaces. When discussing these contexts, a wide range of surveillance technologies and methods was mentioned, including the use of loyalty cards with the aim of monitoring customer behaviour and the use of CCTV systems in order to observe citizens in various spaces. Overall, participants perceived customer surveillance as taking place mainly for security, marketing and advertising functions, while they perceived general citizen surveillance as occurring for reasons of national security and personal safety. Participants were also aware of the extent of surveillance when using a mobile device. This type of monitoring was perceived as occurring primarily for commercial reasons and for security purposes, albeit some expressed their doubts with regards to the latter.

In order to gauge participants' attitudes and beliefs on massively integrated dataveillance, the group was presented with a fictional scenario illustrating the massive integration of data. The possibility of integrated dataveillance occurring was discussed from technical, legal and ethical aspects. Even though opinions varied, most considered this practice as currently possible from a technical standpoint, although not to the extent portrayed in the scenario. Nevertheless, several participants questioned the likelihood of dataveillance and argued that both legal restrictions and ethical considerations would prohibit this practice from taking place. In spite of this, however, it appears that a minority of participants believed that the integration of data is already occurring, albeit in a covert manner. Participants also discussed the acceptability of integrated dataveillance; ethical concerns were underscored by the participants, who mentioned the adverse effect on citizen privacy and the risk that this practice can be employed as a means by the state to exert control over citizens. Additional concerns included the risk of misuse and discrimination. Although the risks of dataveillance were preponderant, a number of positive aspects were mentioned, mainly user convenience, enhanced service efficiency and the provision of free services online. Overall it appears that acceptance was contingent on several factors, including purpose of use, type of data, type of organisation (state institution or private entity) and whether access to data was restricted according to its relevancy to job function.

Participants also discussed the privacy impact and effectiveness of smart surveillance technologies. In relation to the former, participants' opinions were decidedly mixed; while some expressed discomfort at being surveilled irrespective of whether such technologies are fully automatised or else require human intervention, others were rather indifferent. Additionally, some participants perceived automation as impinging less on privacy and thus expressed a preference for smart technologies which do not require human intervention. Opinions were also varied with regards to the effectiveness of the autonomous decision-making capabilities of smart surveillance; while some regarded automatized systems as more objective, others challenged this objectivity since they argued that such systems are nevertheless programmed by humans. On the other hand, several participants appeared to be sceptical of technology on its own without human agency and expressed uneasiness at the risk that smart technologies could erroneously assess or interpret a given situation. In light of this, these participants insisted that the final decision should ultimately rest with a human operator.

During the discussion of the "security-privacy trade off" scenario, while the use of video-surveillance in public places was considered acceptable, the use of surveillance methods involving the physical sphere was met with resistance. Biometric surveillance was generally considered as a threat to privacy, although this appeared to be dependent on context of use; some participants for instance accepted the use of biometric surveillance for forensic purposes. Electronic tagging was considered as extremely invasive and was regarded by some as simply inconceivable. Overall, the use of smart surveillance heightened the participants' sense of vulnerability. In addition to privacy reasons, participants argued that intrusive surveillance could have detrimental consequences on citizen freedom and possibly result in a general criminalisation of citizens. Most rejected the notion that increased surveillance results in increased personal safety and public security and argued that security could never be fully guaranteed. Instead, some advocated the use of education as an alternative to extreme surveillance and control.

Participants were also invited to share their viewpoints on surveillance legislation. Firstly, a lack of knowledge vis-à-vis the content of the legislation was apparent amongst some of the participants. Regarding the effectiveness of the legislation, opposing views were evident; while some stated that they feel protected, several others argued that no legislative mechanism could ever be fool proof. Moreover, others pointed out that the real issue lies with whether the legislation is enforced. Participants proceeded to suggest a number of legal safeguards in order to protect citizens' privacy, including providing citizens with a log of who accessed their data at regular intervals. Lastly, in relation to the length of storage, expectations were varied and appeared to be contingent on type of data.

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, 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 Slovenia is University of Ljubljana (UL).

Focus group discussions were conducted in a total of 14 countries and this document provides the findings from the study that are relevant to Slovenia. Other separate reports are available for Austria, Bulgaria, Czech Republic, France, Germany, Italy, Malta, Norway, Romania, Slovakia, 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 project. The focus groups in Slovenia were carried out on the 1st April, 2013; 15th April, 2013 and 16th April, 2013[2]. The composition of the groups held in Slovenia is described further on 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 fulfilment 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.

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

[2] While Group 2 (25-44 years) and Group 3 (45+ years) were conducted before the Boston Marathon Bombings which occurred on the 15th April, 2013, Group 1 (18-24 years) was conducted the day after the terrorist attack occurred. Although this attack was mentioned during Focus Group 1, in general it does not appear that there were any distinctive differences between the groups.

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 Slovenian 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 between one and a half 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

The data analysis for Slovenia is based on a total of 28 participants with roughly an equal number of males and females in all groups with the exception of Group 2 (25-44 years) in which there were 5 males and 3 females. According to the moderators, the presence of more male participants in this Group appears to have had some effect on the female participants, who were described as being reserved during the discussion. As also mentioned earlier in Section 3.1, in addition to recruiting an equal number of males and females it was also desirable to recruit participants with a diverse educational level and occupational status. In the case of Slovenia, it should be noted that in Group 1 (18-24 years) and Group 2 (25-44 years) a substantial number of participants had a technical background; most of the participants in Group 1 were students reading for different degrees in the field of Electrical Engineering, and, similarly, several participants from Group 2 held a degree in Electrical Engineering. In contrast, the participants belonging to Group 3 (45+ years) had different occupational backgrounds, including technical and non-technical backgrounds. This is being highlighted since in certain parts of the discussion it is evident that some of the participants have a rather detailed knowledge of different smart surveillance methods and technologies.

The composition of all three groups is depicted in the following table:

Participant number	Group 1 – 18-24 years	Group 2 – 25-44 years	Group 3 – 45+ years
P1	M	M	M
P2	M	M	M
P3	F	M	F
P4	F	M	M
P5	M	M	F
P6	F	F	F
P7	F	F	F
P8	M	F	M
P9	M	-	M
P10	F	-	M
Total	**10**	**8**	**10**

The atmosphere in Group 1 (18-24 years) was described by the moderators as formal and cooperative. While some participants appeared reserved or even slightly anxious, one of the participants (P3) was more talkative than the rest of the group. When compared to the other two groups, the overall flow of the discussion was not as smooth and according to the moderators, these younger participants easily changed their position if someone more dominant in the group expressed a different but more strongly defended opinion.

The atmosphere in Group 2 (25-44 years) and Group 3 (45+ years) was described as friendly and relaxed and the overall flow of the discussion was smooth and free-flowing. Some of the participants in Group 2 were regarded as especially cooperative and enthusiastic. A number of participants from both groups (P2-II, P3-II, P1-III and P9-III) were described as being particularly dominant and talkative.

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: *"They can watch you all the time in the supermarket"* (7-III). The use of loyalty cards and CCTV systems were perceived as the predominant methods through which consumers are monitored, while less frequently mentioned methods of surveillance included financial monitoring. In addition, a small minority of participants suggested the possible use of smart technologies.

Surveillance in this context was perceived as being primarily directed at monitoring overall patterns of consumption rather than at the individual consumer: *"I think that in a supermarket it is not so much about the individual but more about all consumers"* (P10-I). Loyalty cards were perceived as enabling commercial establishments to gauge consumers' purchasing power and to analyse consumer behaviour and shopping habits. Main perceived purposes were therefore related to advertising and marketing functions: *"If you're looking for the optimal position in a store for a specific product […] or how to advertise"* (P3-I). In fact, the collection of customer data was perceived as a lucrative practice for commercial establishments: *"[…] because once you have this information you can derive a lot from it, anything you want to know […]"* (P1-I). Some participants also suggested that customer databases are developed by integrating the various data collected from different monitoring methods:

> *"If you look at the receipt, it is very accurate, you can see the timing when you bought and if you pay by card, and all this can be connected. In this way the database can be formed, allowing them to see for example what some customers buy, when and how much. I think that the bar code is not only to track and optimize stock, but it is also, somehow in some indirect way, for gaining some information on buying habits, preferences, and so on […]" (P2-III).*

Video-surveillance was regarded as being used for security-related reasons, mainly for the investigation of crime such as theft. In this regard, some were quick to point out that the commercial establishment was solely safeguarding its own interest: "*They have video-surveillance for themselves and not for the customers"* (P5-III). The use of cameras was generally perceived as having an investigative function rather than a preventive one in real time:

> *"I cannot imagine that they have a security guard and he's looking at some 20 screens and is able to see that someone stole something. It is impossible. I think that it works more like this; that if they find that something is missing then they will look at the recordings, otherwise they wouldn't. It seems unrealistic to me that someone would monitor all actions in the supermarket" (P2-II).*

Although most participants regarded video-surveillance as being utilised primarily for security purposes, some did not exclude that cameras could additionally be employed for the monitoring of consumer behaviour: "*There are many things that can be done using cameras, for example to study where someone stays longer or which shelves are most popular" (P2-II).* Moreover, a minority of participants underscored the risk that surveillance data, particularly video-recordings, could be misused: *"Anyone who is a big shot could have access to these recordings and could do anything they want"* (P3-I).

In addition to the aforementioned monitoring methods, a minority of participants hinted at the possible use of smart technologies, such as *"a sort of transmitter"* installed on shopping carts: "*I do not know exactly how it is done. You can actually record someone's face to determine whether their eyes are down or in a more neutral position or looking up"* (P3-II). Although others also mentioned smart surveillance such as RFID technology, CCTV with Automated Face Recognition (AFR) and gait analysis, they did not expect such technologies to be currently in use at supermarkets: *[…] supermarkets probably don't use that since there is no need and probably no funds. In the future it will probably go in this direction"* (P8-III). Nevertheless it should be noted that these particular views may be a result of the high level of technical knowledge of these particular participants, and therefore such views may not be shared by the population at large.

5.1.2 Boundary Space

In the context of border control, the discussion mainly focused on an airport setting as a boundary space. Surveillance when travelling on land and at border crossings was also briefly discussed by the participants in Group 1 (18-24 years). Overall, surveillance in boundary spaces was considered as ubiquitous and as occurring through a variety of methods: *"The possibilities are endless"* (P5-I). Participants perceived national security and passenger safety as the predominant purposes of surveillance at airports. In general it appears that surveillance in this context was perceived as thoroughly justified: *"It seems to me quite logical that when you enter a foreign country by plane they check you and put you in the system […] I have no problem with that"* (P5-II). Consequently, participants argued that the benefits outweigh the inconvenience caused to passengers and the impact on privacy: *"This causes more benefit than harm. In order to let them catch someone who does not have good intentions, we sacrifice some of our privacy, to feel safer"* (P3-II). In addition to security purposes, albeit to a much less extent, a minority of participants briefly mentioned marketing purposes as another function of surveillance.

In line with the pervasiveness of surveillance in this context, a variety of surveillance methods was mentioned by the different groups. The use of video-surveillance and biometric technologies such as fingerprinting and retinal scanning were perceived as common at airports. Participants also mentioned a number of object and product detection devices, such as luggage scanners, x-ray machines and sensors which are able to detect dangerous substances such as explosives. The monitoring of personal data via the purchase of flight tickets, at passport control and through visa applications was also discussed. A minority of participants also mentioned financial monitoring: *"When we pay with a credit card we all leave tracks"* (P2-III). One participant who appeared rather knowledgeable about the topic also alluded at the massive integration of data from different databases: *"[…] they collect data using several systems"* (P2-II). In addition to technological surveillance, some participants also mentioned the use of sniffer dogs. In addition to the airport authorities, participants were generally aware of being surveilled by a variety of other entities, including commercial entities such as travel agencies, different local government authorities such as law enforcement agencies as well as foreign governments.

In relation to surveillance while travelling on land, which was discussed solely by participants in Group 1 (18-24 years), mention was made to the use of Automatic Number Plate Recognition (ANPR) cameras on roads and at border crossings, which were perceived as being utilised for speed limit enforcement purposes and for the payment of tolls respectively.

5.1.3 Common Public Spaces

In common public spaces, such as museums, underground or train stations and stadiums where mass events are organised, participants mainly mentioned video-surveillance as the primary means of monitoring citizens. In addition to technological surveillance, reference was also made to the presence of security officers and law enforcement personnel, including plain clothes police officers.
The predominant function of video-surveillance in public places, especially where large numbers of people gather, was perceived as being public security and citizen safety: *"In the case of a large crowd, cameras might be used. Cameras track the movements of people and therefore could help in the case of crowded places, for safety reasons"* (P2-I). In this regard, participants discussed two main functions, namely the prevention and investigation of incidents. In relation to the former, a main preventive function was that related to the monitoring and control of crowds during events:

> *"[…] at the stadium supporters could be monitored to prevent them from running to the, let's say football pitch. If everything is recorded and you have algorithms that somehow filter the whole happening, you can say there is a potential danger and direct security guards there" (P2-III).*

Additionally, some participants perceived surveillance during sports events to occur for the timely identification of known or suspected hooligans, so that necessary action could be taken. In this case, some participants mentioned that data on known offenders could be shared even between countries in order to avoid incidents of hooliganism. In relation to the investigation of any incidents, others

mentioned that surveillance data would be stored and could thus serve as evidence: *"If it turns out that there is any need, let's say something happens, someone could check the recordings afterwards"* (P1-I). Lastly, with particular reference to museums, some participants mentioned the use of surveillance for the protection of property and artefacts.

5.1.4 Mobile Devices and Virtual Spaces

Participants from all groups appeared to be aware of the extent of surveillance when making use of a mobile device and mentioned a range of methods through which technologically-mediated surveillance occurs, or can potentially occur, within this context. The most frequently mentioned method was location tracking through GPS: *"An individual can be traced to a few meters accurately"* (P2-II). Other commonly mentioned methods included the monitoring of call and message lists, the recording of conversations, and the collection and sharing of data via the use of smart phone applications: *"Practically every application on the smart phone sends data, GPS location. A lot of information is being exchanged"* (P2-I). For some participants, the latter was considered as rather intrusive: *"It bothers me. Once I wanted to download an application, which was quite basic, but it required access to the entire phone. Sometimes I decide not to download such applications"* (P7-II).

In general, it can be noted that surveillance data in this context was perceived as being used for two main purposes. Firstly, some participants mentioned the use of data for security-related purposes although others were sceptical and mistrustful with regards to the actual purposes of data collection in this regard: *"I think that almost all of this is already misused. They emphasise that data should be collected for security purposes, but is it really only for safety or is it for something else? This is the question"* (P2-II). Secondly, commercial reasons were regarded as being paramount by some participants *"I think money is behind everything"* (P4-II). Surveillance data was considered as valuable for marketing and advertising purposes, and the collection of data was thus perceived as a lucrative practice: *"Once they get that information, they can sell it"* (P2-I). Specifically in relation to the virtual space, a number of participants from Group 2 (25-44 years) mentioned the customisation of content, which they appeared to find useful:

> *"I certainly do not mind if it is [used] for marketing purposes. For instance if it has an algorithm in the background on an online store that keeps track of my purchases and then it can suggest what could be interesting for me or [else] remove the things that are of no interest to me […] in principle I have no problem with such systems" (P5-II).*

In addition to the aforementioned mistrust in relation to private and commercial enterprises, some participants felt that citizens were exposed and vulnerable "*due to the fact that almost everyone has a phone in their pocket almost all the time"* (P5-I). Lastly, it appears that this vulnerability was, in part, due to the perception that as citizens they are relatively uninformed about the myriad of surveillance practices possibly occurring in this context: *"We are often not even aware of the possibilities that already exist"* (P3-I).

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"[3]. In order to elicit the attitudes of the participants, participants were presented with an everyday scenario: a recorded telephone conversation between a job seeker and a civil servant of the employment agency, where complex surveillance[4] becomes evident.

5.2.1 Feelings

After having listened to this *"creepy"* (P6-III) scenario, some of the focus group participants revealed feelings which were of a rather passive nature. Predominantly it appears that an extreme sense of discomfort was felt by these participants, who described feeling *"horrible"* (P7-I) and *"uncomfortable"* (P6-1) at the idea that so much information is known about them. In addition to discomfort, others stated that they would feel surprised should they experience such extensive data collection: *"I would ask myself why all this is needed"* (P2-II).

5.2.2 Behavioural Intentions

In addition to asking about their feelings, a number of participants were also asked for their resulting behavioural intentions. While some participants claimed they would have questioned the civil servant about how their personal data was obtained: *"I would ask her how she knows all that"* (P6-II), others stated they would cut off all communication with the state agency. In general it appears that most reactions were of a rather passive nature.

5.2.3 Beliefs

5.2.3.1 Likelihood of smart surveillance and integrated dataveillance

Regarding whether smart surveillance and massively integrated dataveillance are possible (currently or in the future), the focus group participants generally distinguished between technical, ethical and legal aspects. Generally, the development of massively integrated dataveillance was perceived by most participants to be *"technologically quite possible"* (P2-I), albeit not to the extent as portrayed in the scenario, which was considered by some as rather extreme: *"But not this way, it is still a bit too exaggerated"* (P5-I). Nevertheless, some participants in Group 3 (45+ years) pointed out that this kind of

[3] Clarke, R. (1997)

[4] 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.

intrusive surveillance is not a recent phenomenon but one which already existed decades ago, even without the presently available technologies: *"Surveillance has been in existence since ancient times, only by other methods"* (P1-III). Additionally, in relation to technical capability, it appears that the massive integration of data was perceived by some as a rapidly evolving practice occurring in other countries, particularly the US, but not in Slovenia: *"We are, however, behind them"* (P3-I).

Nevertheless, although technically possible, several participants questioned the likelihood of massively integrated dataveillance from both a legal and an ethical perspective: *"This cannot happen since it is not acceptable in society and it is also not legal. I think that currently there are enough obstacles that prevent this from happening"* (P3-II). More specifically from a legal aspect, some participants mentioned that the Information Commissioner would prohibit this from happening. However, a minority of participants argued that in spite of legal provisions, the massive integration of data from different sources is already occurring in a mostly covert manner: *"In my opinion it's already happening, we are just not aware [of it]"* (P7-II). Additionally others did not exclude the possibility that future legal developments could result in such practices becoming permissible.

5.2.3.2 Acceptance of smart surveillance and integrated dataveillance

After discussing the likelihood of massively integrated dataveillance, the participants also discussed its acceptability. As mentioned previously, participants generally regarded the scenario as unacceptable due to privacy reasons. At the same time, however, some argued that surveillance is, to a certain extent, undergoing a process of normalisation, especially in certain spaces, such as in the virtual space.

Overall it appears that participants' acceptance of massively integrated dataveillance depended on different factors, including purpose of use: "*The question is for what purpose the information is collected"* (P6-III). Another related aspect which had a bearing on the acceptance of dataveillance was the type of data to be stored and shared. Although there were slight differences in the opinions of participants, some general trends emerged. Overall, it seems that while participants did not mind divulging their most basic details including name, surname, gender and address, they did object to the sharing of personal data such as habits, location, financial information as well as medical and health data, which they considered as particularly confidential. In general it was argued that such data should not be shared between entities and that use and access to such data should be restricted "*only to those that need to know [this data] because of their role"* (P2-III), as explained by the following participant:

> *"Your doctor monitors your condition, this is not a problem - there is no fear that you would reveal too much information to the doctor. If, however, a civil servant at the tax office would monitor your health status, this is unacceptable" (P9-I)*

In addition to privacy reasons, this was also perceived as unacceptable due to possible risks of misuse as well as the fear of being discriminated against, such as in an employment context. Nevertheless, it

appears that in specific situations, especially in potentially life-saving circumstances, the use of certain types of confidential data, such as medical data and location-tracking, was considered as justified:

> *"It depends on the situation. For instance I do not want someone to know that I'm going on a trip to Sri Lanka, but if there's an earthquake I would be very glad if an embassy or whoever takes care of Slovenian citizens [in that country] would try to find me and determine whether I am alive or not" (P6-II).*

In relation to potential usage of data, some participants additionally stated that data collection could be helpful with regards to statistical analysis. Moreover, dataveillance was also perceived by some participants as acceptable in cases where it was considered as resulting in the provision of free services, such as free search engines on the internet, and also in cases where dataveillance was regarded as enhancing service efficiency and facilitating user convenience: *"In a way it is kind of handy, isn't it?"* (P4-I). Nevertheless, some participants were keen to point out at a number of risks, in particular that data could potentially be used for *"malicious purposes"* (P1-II) though they did not elaborate further on this.

Lastly, participants discussed their attitudes towards the collection, use and sharing of data by the state and by commercial enterprises. Attitudes on this issue were noticeably mixed; whereas some participants were of the opinion that the state was more trustworthy in this regard: *"The state administration will gather information in order to help me, while private entities will help me to empty my wallet"* (P9-III), others did not show much trust in the authorities: *"I would even say that I have a major problem with the state rather than with the private sector"* (P1-III). It appears that the latter views in relation to the collection of data by the state were due to a number of reasons. Firstly, extensive surveillance was considered as a possible means for the state to exert control and power over citizens: *"The state can control public opinion. If a state has people's [personal] data they know how to plan propaganda […] so they can manipulate you*" (P4-I). In this respect, the mere idea of a centralised data storage system was considered as *"most dangerous"* (P10-III) and resulted in feelings of vulnerability amongst some of the participants: *"God forbid we combined the data into one system, because it would be really powerful"* (P3-II). Additionally another participant, underscoring the political aspect, pointed out that in times of political instability, the collection and storage of surveillance data by the state could result in detrimental consequences for citizens:

> *"In my opinion whether you trust or don't trust the state with your data, this would mainly depend on the situation in the country. If a country is in a state of disarray, then you do not even know who has control, and therefore you would not want to trust […]" (P3-I)*

In relation to the private sector, overall participants expressed a lack of trust: "*The private sector can probably be somewhat limited by law, but anyway, I think that there is a higher possibility of abuse"* (P2-II). Due to commercial motivations, some participants additionally argued that despite legal restrictions, such entities are inclined to do as they please: *"In the case of the private sector, such as commercial companies, if you're lucky they will follow the rules and will use the data only for the purposes that they told you"* (P2-III). Nevertheless, one participant emphasized the citizen's self-responsibility in this

possible misuse: *"We give them [private entities] information by ourselves and then they can use it [although] I don't know how. We are often naïve*" (P7-III).

5.2.3.3 Perceived privacy impact and effectiveness of smart technologies

Participants also discussed the privacy impact and effectiveness of smart technologies. With regards to the perceived impact on privacy by automated systems, a range of opinions could be observed. Some participants appeared to feel discomfort when monitored by surveillance technologies, irrespective of whether such technologies are fully automated or require the intervention of a human operator: *"In both cases you feel uncomfortable"* (P10-I). Others expressed a preference for automated systems: *"Well I feel less uncomfortable if I am observed by automated systems"* (P4-I) and expressed their discomfort at being observed by human operators: *"I would feel uncomfortable with the fact that someone is staring at me"* (P3-III). Additionally, several others expressed indifference: *"I do not care"* (P8-II) or else claimed that *"it does not matter"* (P7-I) since individuals are generally unaware of whether surveillance technologies are wholly automatic or manned by humans: *"We may not realise that this is happening"* (P6-II).

Participants also discussed the automatic decision-making process of smart technologies. It appears that the issue of automation brought up mixed feelings and beliefs amongst the participants. Firstly, the participants differentiated between decisions taken by humans and those taken by automated technologies. In this regard, it appears that a number of participants perceived the decisions taken by automated systems as being objective since there is no human agency involved. These participants argued that humans, unlike machines, introduce an element of subjectivity due to their feelings and judgements: *"The device itself is insensitive to emotion while people are not"* (P4-II). However, this viewpoint was challenged by some participants who argued that such systems are nevertheless programmed by humans: *"the logic has to be written by man"* (P7-I). Therefore, human biases were understood as being transferred to the machine through the programming process thus creating a blurred line between "human" and "machine".

On the other hand, others appeared to be sceptical and distrustful of technology on its own without human agency: *"Big brother is not smart enough"* (P5-I). These participants expressed their unease at the risk that smart technologies could erroneously assess or interpret a given situation: *"These systems do not have a sense of humour and they can come to wrong conclusions. I see this as a bigger problem"* (P1-II). Moreover, some participants also pointed out that one of the downsides of wholly automated systems is that there can be no negotiation in such circumstances: *"You cannot talk to the system and explain the situation. After all, we can get to the point that you're completely isolated from society"* (P9-II). Hence, some participants argued that the final decision should ultimately rest with a human operator: *"I think that at the end [of the decision-making process] there must be an operator who decides or confirms"* (P8-I).

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 participants. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging of vulnerable groups. 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[5].

When discussing the scenario, it appears that participants predominantly perceived the use of the aforementioned surveillance measures as particularly excessive and as *"exaggerated"* (P5-I). Participants from the different age groups argued that with the introduction of extensive surveillance, a democratic state could easily develop into a totalitarian regime: *"[…] such control gives the possibility to the leaders to transform the country into a police state"* (P8-I). In fact, rather than enhancing feelings of personal safety, the surveillance measures portrayed in the scenario resulted in feelings of discomfort and insecurity amongst most of the participants: *"I think that this would not help to improve the safety [of citizens]. I think this would be too invasive"* (P2-II). Nonetheless, a minority of participants did claim that increased surveillance would increase their feelings of safety: *"I would feel safer because there is a higher possibility that the perpetrator would be found"* (P6-I).

A number of reasons can be attributed to the increased sense of insecurity and vulnerability felt by most of the participants. Several participants expressed concern at the way that surveillance measures violated their privacy since *"every step is observed"* (P5-I): *"I would not feel safe, because in addition to [knowing everything about] these suspicious guys, they [the police] would also know everything about me and I do not like that"* (P10-I). While for these participants privacy was considered as more important than security, there were others who in addition revealed further concerns. In particular, the use of extensive surveillance was perceived as providing a pretext to exert control over citizens: *"But it's just an excuse for the state to assume greater control"* (P8-III). Participants also argued that such a scenario would be conducive to creating the ideal conditions for controlling citizens: *"It allows easier control of the people and therefore, they might use it for their own purposes, and that does not seem right to me"* (P8-I). Due to this belief, some participants also appeared concerned that the focus of surveillance could shift from monitoring criminals to observing all citizens:

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

> *"I think this is a bit exaggerated. Taking DNA, fingerprints from all. Nowadays they usually take the fingerprints from every criminal. It doesn't seem right that everyone's fingerprints are collected. This should be only for identifying former criminals […] (P1-I).*

Some participants also mentioned possible repercussions that this type of extensive monitoring could have on individual behaviour: *"Yes, you cannot be relaxed in this case. You are careful all the time, even if you don't have any bad intentions […] you are in fear all the time because you think everyone is watching you"* (P10-I). In addition to the controlling function of surveillance, some participants suspected that other ulterior motives, such as commercial interests, could be behind the introduction of these technologies: *"I would ask myself whether this system is introduced in order for someone to [financially] profit from it. I don't think it is there to protect me"* (P6-III).

Another factor which appeared to heighten the participants' sense of vulnerability was the possibility that personal data collected by smart surveillance would be misappropriated or misused: *"I think it is a short step to misuse and that scares me"* (P7-III). Some participants seemed particularly concerned about the risk that evidence could be fabricated thus resulting in an innocent individual being wrongfully accused:

> *"I do not know if I would trust them. The data could be abused. What would happen if they find my DNA somewhere, would that be enough to convict me? […] It seems to me that someone could abuse this let's say by placing your DNA somewhere" (P5-II).*

Hence, some participants emphasised that rather than the actual collection of citizen data, the real difficulty lies with preventing possible misuse: *"The problem I see is how these data are processed and how they are protected. The biggest problem is how the law is respected or how the state will act to prevent misuse of these data"* (P6-I). In light of this concern, several participants pointed out that the acceptability of such a surveillance system would be contingent on the way the data is managed: *"As long as this is for security purposes and you know that these data are handled properly, that they are not shared and that the access is limited, then this seems to me somehow acceptable"* (P1-I). Nevertheless, some participants expressed their reservations with regards to the security of any system: *"[…] even if you control everything there are still flaws"* (P3-I).

In spite of a marked increase in crime portrayed in the other versions of the scenario, participants were still of the opinion that extensive surveillance measures could not be justified, with only a minority expressing their confidence in surveillance measures and a corresponding willingness to sacrifice their privacy following an increase in crime: *"I think that we agree with almost everything when such incidents occur. Even if I say no now, if I would be really scared, I would agree with many things. Even if they would tag me, it would be fine with me"* (P6-II). It also appears that the opinions of some of the participants from Group 1 (18-24 years) might have been slightly influenced by the Boston Marathon bombings, which happened only a day prior to this focus group. In particular, one participant, who made reference to this terrorist attack, expressed her confidence in surveillance technologies:

> *"I think that in the future this technology will have an effect on safety, it will increase safety. For example just yesterday the bomb exploded at the Boston Marathon. With more control and action maybe such incidents would not happen or at least less damage would occur" (P6-I).*

While these participants appeared to appreciate the caring function of surveillance, the majority showed a rather cynical attitude towards the use of surveillance, with some arguing that increased surveillance creates *"a false sense of security"*: *"[…] All of a sudden we have a feeling that everything is safer because it is controlled and we are not careful […] this is counter-productive"* (P9-III). In line with this, a number of participants doubted and challenged the notion that technological surveillance was the best solution to reduce or eliminate crime since the use of surveillance was regarded as *"a false solution"* (P4-III) given that it *"deals with the consequences and not with the causes"* (P8-III). In fact several participants argued that *"these problems should be addressed differently, not with [the use of] technologies"* (P4-I); here, some participants, mainly from Group 1 (18-24 years) and Group 3 (45+ years) mentioned the use of education as an alternative to extreme surveillance and control:

> *"I think that observing and controlling people is not a long-term solution for obtaining safety, if such a system is established for that purpose. A long-term solution is that there should not be such control, for instance a different approach could be used in kindergarten already, so education should be different. I think we will eventually become, if this different education does not happen, really just numbers with name and surname. This scares me and I think this will happen" (P9-I).*

Although most participants acknowledged that the use of technology could be useful for purposes of investigation*: "[…] if all this is done, this could be done only to make investigation easier. As for prevention there would be no difference"* (P1-II), some participants were quite keen to point out that criminals could evade surveillance: *"[…] it seems to me that criminals are always a step ahead"* (P1-II). Thus, in terms of prevention, most technologies were regarded as being simply futile:

> *"Well, it seems to me that it is wrong to invest the money into such technologies. The problem of these technologies is that they do not prevent crime, they help to solve a crime faster but they do not prevent crime" (P8-I).*

5.3.2 Perception of Different Technologies

In general, different types of surveillance technologies seemed to meet different levels of acceptance. The use of video surveillance was on the whole considered as generally acceptable in public places such as in streets and on public transportation systems: *"I think it's a little more acceptable if it's just for public spaces"* (P8-I). Nevertheless, some participants did object to being monitored in certain public places, especially in places where people usually go to unwind or else to engage in leisure activities: *"What about the park? Is it meant as a public place? If you are running there, how would you feel if you know that someone is watching you? Or if you are having a picnic?* (P3-I). With regards to private spaces,

including one's home, surveillance in such contexts was considered as totally unacceptable: *"They are already in public places and I do not mind. As long as they are not in my apartment or in some other private premises […]"* (P6-II). Moreover, a number of participants expressed their discomfort at being surveilled in the changing rooms of commercial establishments and public conveniences.

While few participants objected to video-surveillance, the use of biometric data and electronic tagging – hence surveillance involving the physical sphere – was in general considered as not acceptable. Overall, the collection of this type of data was perceived as presenting a higher threat to privacy. Nevertheless, some participants who were generally opposed to the use of biometric surveillance did appear to accept such use specifically for forensic purposes:

> *"Let's say biometric data, it seems acceptable to me. Mainly due to the fact that if they would investigate a crime, biometric records would help them to find the perpetrator and additionally, people would think twice before doing anything" (P8-I).*

Lastly, the use of electronic tagging provoked an even stronger reaction than biometric surveillance; perceived as *"too invasive"* (P9-III), this surveillance method was regarded by some participants as simply inconceivable: *"That they would insert a chip somewhere, I cannot imagine it"* (P6-II). It appears that participants generally objected to the tagging of elderly people and especially to the tagging of children; here some questioned whether this would have a negative effect on children's development: *"How would this affect the children's psyche, if they know they are under control? Would this affect them later on?"* (P3-I). Others also expressed their disagreement with regards to the tagging of criminals: *"It seems more acceptable if we mark criminals, since they already did something which is not ok, but still I find that unacceptable"* (P3-II).

5.4 Surveillance Laws & Regulations

During the last part of the focus group sessions, issues relating to surveillance laws and regulations were discussed including participants' familiarity with privacy legislation, effectiveness of legislation and trust in the state, and lastly, length of data storage.

5.4.1 A lack of information or nonchalance?

During this part of the discussion, a lack of knowledge and initiative vis-à-vis the content of legislation was evident from the outset amongst some of the participants who for instance claimed *"I cannot comment because I don't know what the law states"* (P5-I). While some participants explained this lack of knowledge by arguing that there are not enough initiatives aimed at raising awareness and educating citizens about privacy rights, others argued that the problem is that citizens are simply not interested: *"The problem is that people do not care"* (P9-III).

5.4.2 Effectiveness of legislation

Participants had rather varied opinions with regards to the perceived level of protection offered by the state. Some participants expressed their faith not only in the legislation: *"The law protects us"* (P9-III), but also conveyed their trust in the function and endeavours of the current Information Commissioner: *"I think she [the Information Commissioner] is quite active and strict and therefore, I feel safe"* (P5-II). On the other hand, others argued that no legislative mechanism could ever be fool proof: *"The problem lies with the fact that there is still a possibility to circumvent […] it is hard to draft something that would not be possible to get round*" (P3-I).

However, others suggested that the problem does not lie with the legislation as such and argued that the crux of the issue is whether the legislation is respected or not: *"The legislation exists. The question is, if they are abided by and what happens if they are not. You don't feel safer only because the legislation is in place, what matters is what happens then"* (P7-I). Hence it appears that for these participants, their foremost concern was related to the enforcement of the legislation, or lack thereof: *"The law protects us but how it is implemented does not [protect us]"* (P9-III).

5.4.3 Suggested safeguards

Participants were also asked about possible legal and procedural safeguards the state could introduce in order to protect citizens' privacy vis-à-vis the massive integration of data. A number of suggestions were proposed by the participants, including informing citizens with whom their personal data was being shared and for what purpose. More specifically, some participants suggested that *"a log of people accessing the database"* (P4-III) should be kept by the state and duly provided to citizens on a regular basis:

> *"If the state would really collect all this information, I would like to have control over who accessed the data. Let's say that I would be informed about everything. Each citizen would have an account, where you would see what is happening with your data, and that should be everyone's right" (P1-II).*

This was perceived as providing citizens with the opportunity to monitor those entrusted with administering their personal data, thus resulting in a situation where the subjects of surveillance in turn monitor, to a certain extent, their surveillants: "*Just like someone can watch you, even if this person is an authorised person, you can also watch them, or at least you can watch that this person is watching you"* (P1-II).

5.4.4 Length of data storage

The expectations of participants regarding the storage of their private data were rather varied. Whilst some participants deemed storage period to be irrelevant, others declared that this made a difference to them, and proceeded to provide numerous time spans which they believed would be appropriate. In general, while some participants argued for a very short time span: *"As little as possible, I do not know, a week, a month. One week is quite sufficient"* (P9-III), others suggested that a longer duration would be more appropriate: *"I think we should talk more in terms of years"* (P1-I).

Additionally, it appears that for some participants, storage period was dependent on type of data. While in the case of location data some participants argued for a short storage period *"location data should be deleted after a week or a month"* (P8-I), it appears that where biometric data was concerned, participants preferred a longer duration: *"I also think that, for example DNA should be stored for a longer time, since it is the same for your whole life. Fingerprints also don't change rapidly, while photos can change much faster"* (P1-I).

6. Conclusion

Slovenian participants displayed a high level of awareness that individual citizens are indeed the subjects of surveillance in commercial, boundary and public spaces. The results indicate that surveillance in these spaces has undergone a process of normalisation and participants do expect that surveillance occurs in such contexts. Technologically-mediated surveillance was regarded as generally acceptable for security-related purposes in all three spaces as well as for marketing purposes specifically in commercial spaces. On the other hand, it appears that surveillance via the use of mobile devices resulted in feelings of vulnerability for some participants who felt particularly exposed due to the often unknown nature of surveillance occurring through such means.

The majority of participants believed that massively integrated dataveillance is undoubtedly technically possible; at the same time, however, most were of the opinion that legal restrictions and ethical considerations would prohibit the massive integration of personal data. Nevertheless a minority of participants believed that this practice is already taking place, albeit in a covert manner. Integrated dataveillance was generally considered as unacceptable on a number of counts including the adverse effect on citizen privacy, the risk of misappropriation and misuse, as well as the possibility that dataveillance could be utilised by the state as a tool to exert control and power over citizens. Only a few positive aspects relating to dataveillance, such as user convenience, were mentioned by the participants; in this regard they conveyed the double-edged sword nature of surveillance: *"This is a catch-22 situation"* (P1-III). Overall it appears that acceptance of this practice was contingent on a number of factors, including purpose of use, type of data, type of organisation conducting dataveillance and the existence of restrictions to data access.

Views on the privacy impact and efficiency of smart technologies were varied. Some participants expressed discomfort at being surveilled irrespective of whether such technologies are fully automated or else require human intervention. Additionally, others perceived automation as impinging less on privacy and thus expressed a preference for technologies which do not require the involvement of human operators. Moreover, a number of participants argued that individuals are generally unaware of whether surveillance technologies are wholly automatic or manned by humans, and thus expressed indifference as to whether the surveillance process was automated or else included human intervention. In relation to effectiveness, several participants regarded automated systems as more efficient due to the belief that the decision-making process of such systems would be devoid of human biases and thus more objective. In contrast, others were sceptical of the use of technology on its own without human agency and expressed unease at the possibility that smart technologies could erroneously assess or interpret a given situation. Human agency was thus deemed as a crucial element in the decision-making process of smart surveillance.

Surveillance was ascribed both a 'controlling' and a 'caring' function by the participants, with the former being much more pronounced than the latter. It appears that most Slovenian participants questioned

the use of extensive surveillance for the sake of security, especially since they argued that security could never be fully guaranteed. While most participants acknowledged that surveillance technology could be useful for purposes of crime investigation, it appears that in terms of prevention, they regarded the use of surveillance technology as rather futile. Moreover, the possibility that personal data could be misappropriated or misused was perceived as a very realistic threat amongst participants and seemed to cause a high level of unease. In light of these beliefs, most participants stated their reluctance to sacrifice their privacy for increased surveillance. Nevertheless, a minority of participants felt reassured with the presence of surveillance measures and it appears that increased levels of surveillance provided them with a sense of safety; they thus seemed more willing to sacrifice their privacy following an increase in crime.

With regards to surveillance laws and regulations, a lack of knowledge vis-à-vis the content of the legislation was apparent amongst some of the participants; while some proposed that this is due to a lack of initiatives aimed at raising awareness on citizens' rights, others argued that citizens are simply uninterested. Contrasting opinions with regards to the effectiveness of the legislation were evident; while a number of participants claimed that they feel protected by the existing legislation and additionally expressed their trust in the current Information Commissioner, others argued that legislation can, after all, be circumvented. In light of this, a number of participants pointed out that the crux of the matter lies with whether the legislation is effectively enforced or not. Furthermore, as a safeguard, participants stated that those entrusted with administering citizens' data should be monitored accordingly in order to provide a certain degree of transparency.

On a last note, some participants expressed their concerns that the scenarios depicting extreme surveillance are, *"unfortunately"* (P10-I), closer to reality that it seems: *"I have that feeling that we are getting closer to something like this and I do not like it"* (P7-I). Rather than using technology to achieve security, which was deemed as a short-sighted approach that might lead to a sense of de-humanisation were people are considered as *"just numbers with name and surname"* (P9-I), these participants advocated a societal-oriented approach which focuses on education and the development of human relations *"[…] more investment should be made into something that would make man more human"* (P4-III).

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 Commission. 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 discussion*	***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 safety* ***Running Total: 15min***
Discussion on everyday	***Item 2***

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

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?

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

For each item, and where relevant, probe in detail to explore the following:

1. ***How is the information being collected:***
    a. ***Which types of technologies do you think are used to collect your personal information?***
2. ***What type of information is being collected:***
    a. ***What type of personal information do you think is being collected?***
3. ***Who is collecting the information:***
    a. ***Who do you think is responsible for collecting and recording your personal information?***

information is ending up

4. Explore the participants' views on why their actions and behaviours are observed, monitored and collected.

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 the implications of MIMSI*

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

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

***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'...*

Aims

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

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

1. Participants' first reactions including:

Possibility / impossibility of scenario

Acceptability / unacceptability of scenario

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

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

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

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

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?

1c. Is such a scenario possible / impossible?

1d. Is such a scenario acceptable / unacceptable?

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

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

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

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

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

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

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

5b. Do you think there are any drawbacks 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-*

Item 5

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

Due to an significant increase in *violent crimes* in the capital city, including *a spate of kidnappings and murders which seem random and unconnected*, 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

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*

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.

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":

Aims:

1. Security climate and level of threat

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. Deployment of specific technologies

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)

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)* *5. Length of storage of surveillance data*	***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 <u>reassuring</u>?*** ***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 <u>acceptable timeframe</u>?*** ***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	***Item 7 –Closure***

[5mins] ▪ ***Thank the participants*** ▪ ***Hand out the reimbursement*** ▪ ***Give information on SMART***	**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 out more information about the SMART to the participants requesting such information.*** ***Total: 1 hour and 45 min***

APPENDIX C – DISCUSSION GUIDELINES (SLOVENIAN)

Predstavitev	Navodila
Dobrodošlica udeležencem - *Pozdrav udeležencem* - *Razdeljevanje tablic z imeni* - *Podpis izjave o soglasju*	*Dobrodošlica udeležencem takoj ob prihodu. Posedite jih, ter jim razdelite tablice z imeni.* *Razdelite udeležencem izjave o sodelovanju ter jih prosite, da jih preberejo in podpišejo še pred začetkom razprave. To je pomembno zato, ker le tako zagotovimo, da so udeleženci seznanjeni in razumejo s čim se strinjajo.*
Uvod [približno 10 min] - *Zahvala* - *Predstavitev podporne skupine* - *Namen* - *Zaupnost* - *Trajanje* - *Osnovna pravila skupine* - *Kratka predstavitev udeležencev*	**Dobrodošli v tej fokusni skupini in hvala za sodelovanje v današnji razpravi. Veseli smo, da ste si ob vseh drugih obveznostih vzeli čas za sodelovanje pri tem projektu. Vaša udeležba je zelo cenjena.** **Moje ime je _____ in bom vodil/a razpravo v tej skupini. Pri tem mi bo pomagal/a _____ moj komoderator, ki bo zapisoval/a ter snemal/a našo razpravo.** *Predstavite tudi druge sodelavce, ki so morda prisotni.* **Naša razprava bo trajala nekje med uro in pol do dve uri in vas vljudno prosim, da govorite jasno in glasno, saj bomo celotno razpravo snemali. Vaša mnenja in misli so za nas in našo raziskavo zelo pomembna in res ne želimo zgrešiti ali izpustiti kakršenkoli vaš komentar.** **Ko so vas prvič povabili k sodelovanju v tej razpravi, so vam že omenili, da bo ta razprava na temo tehnologije in zasebnosti. Ta raziskava poteka v okviru projekta SMART, ki je sofinanciran s strani Evropske komisije. Za tiste, ki želite izvedeti več o projektu SMART, vas prosimo, da se obrnete na nas po koncu razprave in podali vam bomo več informacije.** *V tej fazi je pomembno, da dodatne podrobnosti o vsebini razprave fokusne skupine niso razkrite, saj se tako izognemo morebitnemu spornemu vplivu na razpravo.* **Kot ste že prebrali v izjavi o sodelovanju, bo vse, kar bo dokumentirano v tekom razprave v tej skupini, zaupno in anonimno. To pomeni, da bodo vaše komentarje prebrali le tisti, ki sodelujejo v tej študiji in da bodo vaši komentarji anonimizirani ter le tako uporabljeni v znanstvenih publikacijah. Na podlagi dokumentiranega vas na noben način ne bo možno identificirati. Da to res lahko zagotovimo, vam bom dodelil/a številko in ta številka bo uporabljena v poročilu.**

	Rad/a bi, da poskrbite, da vam je dovolj udobno in da ste sproščeni, da boste lahko svoja mnenja brez zadržkov delili z vsemi v skupini. Da bi to bilo lažje, bi vas rad/a prosil/a, da upoštevate nekaj osnovnih pravil: ▪ **Zanima nas mnenje vsakega posameznika in zato bi radi slišali vsakega v skupini.** ▪ **Ni pravilnih in napačnih odgovorov, so le različna mnenja in zato vas prosim, da spoštujete mnenja drug drugega** ▪ **Prosim vas, da stišate vaše mobilne telefone in tako omogočite neprekinjeno razpravo.** ▪ **Za nas je pomembno, da naenkrat govori samo eden. Vsako mnenje je pomembno in zato vas prosim, da ne govorite en čez drugega, ker bo v tem primeru težko zajeti vsa mnenja.** ▪ **Da bi se počutili bolj udobno in da bi lažje govorili povsem odkrito, vas prosim, da se zavežemo k zaupnosti.** **Če bi kdo želel predlagati drugačna pravila, vas prosim, da svoje predloge zdaj delite z nami.** **Ali ima kdo kakšno vprašanje preden začnemo?** **Torej, začnimo s tem, da se vsak na kratko predstavi skupini, ne da bi razkril osebne podatke. Naredimo krog in vsak naj pove svoje ime in morda nekaj o sebi. Začel/a bom kar jaz... *(na kratko se predstavite)*** *Pretečeni čas: 10 min*
Cilji	**Teme pogovora ter vaje**
Vaja besednih zvez **[približno 5 min]** - *Z igro besednih zvez pomagati pri prebijanju ledu* - *Vzpostaviti glavne asociacije s ključnimi temami razprave* - *Začetek skupinske razprave*	***Točka 1*** **Najprej se bomo šli eno kratko igro: prebral/a vam bom besedo in rad/a bi da mi poveste nekaj besed, ki vam pridejo na misel, ko slišite to besedo. Poskusimo najprej na primeru: Kaj je prva stvar, ki vam pride na misel, če rečem besedo "hrana"? Razmišljajte o posameznih besedah in kratkih stavkih, izogibajte se dolgim opisom.** *Preberite (po eno besedo):* *Tehnologija, zasebnost, nacionalna varnost, osebni podatki, osebna varnost* *Pretečeni čas: 15 min*
Razprava o vsakdanjih izkušnjah z nadzorom **[20 min]**	***Točka 2*** **Pogovorimo se zdaj o nečem drugem. Rad/a bi, da razmišljate o primerih, v katerih ste imeli občutek, da ste vi ali vaša dejanja opazovana. Pomislite tudi na primere, za katere veste, da se vaši podatki zbirajo. Začnimo s primeri iz našega vsakdanjega življenja.**

- *Raziskati izkušnje udeležencev z nadzorom in kako ga dojemajo*

- *Raziskati ozaveščenost in znanje udeležencev o različnih nadzornih tehnologijah*

Zamislimo si na primer:

Scenarij 1: Supermarket - Za prvi primer se odpravimo na nakupovanje v vaš priljubljeni supermarket. Prosim vas, da delite z nami vaše misli?

Scenarij 2: Potovanje - Kaj pa drug primer, tokrat v povezavi s potovanjem? Kaj pa v primeru, ko potujete z letalom?

Scenarij 3: Javno mesto (npr.: v muzeju, na stadionu) - Zdaj pa si predstavljajte, da ste nekje na javnem mestu, na primer v muzeju ali pa na nekem športnem dogodku ali na koncertu. Kaj mislite, kakšne aktivnosti bi bile opazovane oz. zabeležene?

Scenarij 4: Mobilne naprave - Pa si poglejmo še zadnji primer. Pomislite na trenutke, ko uporabljate mobilni telefon. Kaj mislite, da se beleži v tem primeru?

Cilji:

1. Raziščite ozaveščenost in znanje udeležencev o tehnologijah

2. Raziščite kakšne so izkušnje udeležencev, ko so opazovani v različnih vlogah

3. Raziščite razumevanje udeležencev glede tega, kje njihovi podatki končajo

4. Raziščite mnenje udeležencev glede tega, zakaj se opazuje, zbire ter hrani podatke o njihovi aktivnosti ter obnašanju

Za vsak zgornji primer (in kjer je relevantno) podrobneje raziščite naslednje:

1. ***Kako se zbira podatke:***
    a. ***Katere vrste tehnologij mislite, da se uporabljajo za zbiranje vaših osebnih podatkov?***
2. ***Katere vrste podatkov se zbira:***
    a. ***Kaj mislite kateri osebni podatki se zbirajo?***
3. ***Kdo zbira te podatke:***
    a. ***Kdo mislite, da je odgovoren za zbiranje in shranjevanje vaših osebnih podatkov?***
    b. ***Kje mislite, da končajo vaši osebni podatki?***
4. ***Zakaj se podatki beležijo, zbirajo in hranijo:***
    a. ***Kaj mislite, za kaj se vaši osebni podatki beležijo ter zbirajo ?***
    b. ***Kaj mislite, za kakšne namene se bodo vaši osebni podatki uporabili?***

Pretečeni čas: 35 min

Predstavitev kartic, ki prikazujejo različne tehnologije ter aplikacije
[10 min]

Prikazati udeležencem izbor ustreznih pametnih tehnologij in aplikacij, da jim omogočimo boljše razumevanje ter s tem olajšamo razpravo.

Točka 3

Pokažite skupini naslednje tri kartice (vsaka prikazuje določeno skupino tehnologij in aplikacij). Kartice prikazujejo naslednje:

Kartica 1 – Tehnologije za razpoznavanje in sledenje osebam ali dogodkom: *samodejno premikanje CCTV kamer, sistem samodejnega prepoznavanja registrskih tablic (ANPR oz. AVNI) in naprave za sledenje kot so sledenje mobilnega telefona in RFID*

Kartica 2 - Biometrija*: Biometrične tehnologije, ki vključujejo skeniranje prstnih odtisov ter šarenice in sistem za samodejno prepoznava obrazov (AFR)*

Kartica 3 - Naprave za odkrivanje predmetov in izdelkov*: naprava za detekcijo nožev in rentgen*

Pretečeni čas: 40 min

Predstavitev MIMSI scenarija udeležencem

[30 min]

- *Raziskati razumevanje udeležencev o posledicah uporabe MIMSI*

- *Raziskati stališča, prepričanja in mnenja udeležencev o izmenjavi osebnih podatkov*

Točka 4

Predstavite skupini naslednji zaigrani scenarij. Posnetek telefonskega pogovora se lahko posname vnaprej in se ga nato predvaja skupini.

Telefonski pogovor z zastopnikom za pomoč strankam na javnem Zavodu za zaposlovanje

***Oseba za pomoč strankam**: Dobro jutro, Marija pri telefonu, kako ste g. Novak? Vaš klic smo že pričakovali, saj vam je pogodba o delu pretekla že pred enim mesecem.*

***G. Novak**: Hmm...da, v resnici res kličem zaradi tega ...*

***Oseba za pomoč strankam**: No, jaz pravzaprav nisem presenečena, da ste poklicali ravno zdaj ... kako je bilo na dopustu na Cipru? Prepričana sem, da so vaša žena in otroci uživali v hotelu, kjer ste bivali..*

***G. Novak**: Da, res je bilo lepo na dopustu ... kako pa veste vse to?*

***Oseba za pomoč strankam**: No, vse to je v sistemu, gospod Novak .... očitno. Kakorkoli že, bolje da začnete z iskanjem nove službe ... glede na to, da boste morali kmalu poravnati stroške vašega dopusta ter stroške avtomobila ... da ne omenjam plačila stroškov na vaši VISA kartici, ki vam zapade 22. tega meseca...*

***G. Novak**: Je to tudi v vašem sistemu?*

***Oseba za pomoč strankam**: Seveda gospod Novak. Mimogrede, dobra izbira knjige, ki ste jo kupili na spletu ... Prebrala sem jo tudi jaz in dala mi je res kar nekaj dobrih nasvetov..*

***G. Novak**: Hmm ... v redu ... glede te vaše nove storitve za iskalce zaposlitve, ali vam moram posredovati najnovejšo osebno fotografijo?*

***Oseba za pomoč strankam**: Ne gospod Novak, za to smo seveda že poskrbeli! Imamo veliko vaših novih fotografij. Ravno sem se spomnila ... lepo ste porjaveli na počitnicah! Sigurno je bilo lepo vreme! Predno pozabim, vam je ljubša vaša fotografija, kjer ste z očali ali brez?*

***G. Novak**: Oh ... no .... brez očal bo v redu ... torej, glede moje prijave, ali se lahko dogovoriva za termin naslednji teden?*

***Oseba za pomoč strankam**: Samo da preverim v našem sistemu ... Kaj pa v sredo ob poldne? Oh, počakajte trenutek! Pravkar sem opazila, da imate predviden zdravniški pregled ravno v tem času. Prepričana sem, da si tega ne želite zamuditi, saj je spremljanje vašega holesterola zagotovo pomembno! Kaj pa četrtek takoj zjutraj, ob 09:00?*

***G. Novak**: Četrtek zjutraj bo v redu ... ali moram prinesti s seboj vso dokumentacijo?*

***Oseba za pomoč strankam**: Ne gospod Novak, imamo že vse podatke, ki jih potrebujemo v našem sistemu.*

***G. Novak**: Sem prepričan, da res...*

***Oseba za pomoč strankam**: Hvala za vaš klic gospod Novak in se vidimo naslednji teden. Mimogrede, uživajte v kapučinu v Mestni kavarni...*

***G. Novak**: Jaz sem ...nasvidenje...*

...

Cilji
1. Prvi odzivi udeležencev, ki vključuje:

Verjetnost / neverjetnost scenarija

Sprejemljivost / nesprejemljivost scenarija

2. Prepričanja in stališča udeležencev o tem, kako tehnologije vplivajo ali pa bi lahko vplivale na njihovo zasebnost

3. Prepričanja in

Po predstavitvi zgornjega hipotetičnega dialoga skupini, poskusite poglobljeno raziskati naslednje:

1a. Kako bi se vi počutili, če bi se to zgodilo vam?
(Poskusite določiti tudi kakšno stopnjo nadzora/nemoči občutijo udeleženci v tem hipotetičnem scenariju)

1b. Kako bi se vi odzvali v takem primeru? Kaj bi storili?

1c. Ali je tak scenarij <u>možen / ni možen</u>?
1d. Ali je tak scenarij <u>sprejemljiv / nesprejemljiv</u>?

2a. Kaj mislite, v kolikšni meri posamezne samostojne tehnologije vplivajo na vašo zasebnost?

2b. Kaj mislite, v kolikšni meri vplivajo na vašo zasebnost <u>»pametne« tehnologije</u> – to so tiste, ki vaše podatke obdelujejo <u>samodejno</u> (avtomatsko; ali na pol samodejno - polavtomatsko)?

3a. Za katere osebne podatke se vam zdi <u>sprejemljivo</u>, da se zbirajo, uporabljajo in / ali se izmenjujejo?

stališča udeležencev glede vrste podatkov kot so: zdravstveni zapisi; finančni podatki; fotografije in lokacija.

4. Prepričanja in stališča udeležencev glede zbiranja, uporabljanja in izmenjave osebnih podatkov s tretjimi osebami.

5. Prepričanja in stališča udeležencev o prednostih in slabostih nadzora

3b. Katerim osebnim podatkom bi <u>nasprotovali</u>, da se zbirajo, uporabljajo in / ali se izmenjujejo?

4a. Kaj menite o tem, da vaše osebne podatke zbira, uporablja in izmenjuje <u>država</u>?

4b. Kaj menite o tem, da se vaši osebni podatki zbirajo, uporabljajo in izmenjujejo <u>v zasebnem sektorju</u> (na primer za trženje)?

5a. Ali menite, da je <u>koristno</u>, če so naša dejanja in obnašanje opazovana?

5b. Ali menite, da obstajajo kakšne pomanjkljivosti, če so naša dejanja in obnašanje opazovana ?

Pretečeni čas: 1 uro 15 min

Odzivi na scenarije

[približno 20 min]

- *Spodbuditi razpravo med udeleženci, da bi lažje raziskali dojemanje "kompromisa med varnostjo in zasebnostjo".*
- *Tukaj se razprava ne bi smela osredotočiti na to, ali bodo te tehnologije povečale varnost - to je treba sprejeti kot dejstvo. Razprava se mora predvsem osredotočiti na to, ali ima uporaba teh tehnologij vpliv na zasebnost in zato se vrtite okoli kompromisa med zasebnostjo ter varnostjo.*

Cilji:

1. Varnostna klima

Točka 5

V naslednji vaji bomo razpravljali o naslednjem hipotetičnem scenariju. Predstavljajte si naslednje:

Zaradi porasta nasilnih kaznivih dejanj v prestolnici, vključno s celo vrsto umorov in ugrabitev, ki se zdijo naključna in nepovezana, se je država odločila, da uvede tak nadzor s CCTV kamerami, ki bo omogočal samodejno prepoznavo obrazov v vsakem javnem prostoru, ki je ali v državni lasti (na primer podhodi, parki in javna stranišča) ali pa v zasebni lasti (kot so trgovine, nakupovalni centri in taksiji). Poleg tega se bodo zabeležile vse registrske številke tablic tistih avtomobilov, ki bodo prečkali kontrolne točke. Na vsakem javnem mestu načrtujejo namestitev takih senzorjev, ki so sposobni zaznati glasne zvoke, kot je kričanje. Vsak državljan bo moral oddati svoj DNK, prstne odtise in posnetek šarenice. Država se je prav tako odločila, da bi tiste državljane, ki bi lahko predstavljali določeno nevarnost za druge, elektronsko označili in bi jih na tak način opazovali ter spremljali njihovo gibanje. Tudi starejše ljudi ter otroke do 12. leta starosti bi zaradi njihove varnosti elektronsko označili. Vsi ti podatki, zbrani s pomočjo različnih tehnologij, bodo shranjeni v povezanih podatkovnih zbirkah, ki jih bo upravljala policija in bo v primeru preplaha in nevarnosti za kateregakoli državljana o tem avtomatično opozorjena.

Povejte udeležencem, da si zgornji scenarij zamislijo v naslednjih različicah:

Različica 1: Čeprav je porast nasilnih kaznivih dejanj možno opaziti v večini sosednjih mest, se v mestu, kjer vi živite, ni spremenilo nič. Kljub temu se je država odločila, da nadzor uvede kot previdnostni ukrep.

Različica 2: V celotni državi je na splošno nizka stopnja kriminala, a se je potem, ko se je v sosednjem mestu zgodil incident, v katerem je neznanec streljal v nakupovalnem središču in tako ustrelil ali hudo ranil veliko ljudi, država kljub temu odločila, da uvede tak nadzor kot previdnostni ukrep.

Med razpravo o zgornjem scenariju / različici, poglobljeno raziščite naslednje dejavnike ter njihov možen vpliv na kompromis med "varnostjo in zasebnostjo":

1a. Kaj vam da občutek varnosti v prebranem scenariju?

in stopnja nevarnosti	***1b. Kaj vam da občutek <u>ranljivosti</u> v prebranem scenariju?*** ***1c. Bi bili pripravljeni žrtvovati svojo zasebnost, v primeru če bi bila stopnja ogroženosti drugačna kot v prvi in drugi različici prebranega scenarija?***
2. Uvedba posebnih tehnologij	***2. V scenariju so bile predstavljene pametne tehnologije kot so*** ***CCTV kamere s samodejno prepoznavo obrazov,*** ***samodejno prepoznavanje registrskih tablic (ANPR),*** ***senzorji (sposobni zaznati glasne zvoke),*** ***biometrične tehnologije (vključno s prstnimi odtisi) in*** ***elektronsko označevanje (ki uporablja RFID -*** ***radio frekvenčno identifikacijo)*** ***2a. Katere tehnologije se vam zdijo <u>sprejemljive</u>? Zakaj?*** ***2b. Katere tehnologije so po vašem mnenju <u>vsiljive</u> in predstavljajo grožnjo vaši zasebnosti? Zakaj?*** ***2c. Kaj menite o samodejnih (avtomatskih ali polavtomatskih) tehnologijah, kjer končno odločitev sprejme sistem in ne človek (operater)?***
3. Lokacije uporabe kot so na primer: na letališčih, v nakupovalnih središčih in na ulicah	***3a. Nadzor katerih lokacij (prostorov) je po vašem mnenju <u>sprejemljiv</u>? Zakaj?*** ***3b. Nadzor katerih lokacij (prostorov) se vam zdi <u>nesprejemljiv</u>?***
4. Obstoj zakonov ter drugih zaščitnih ukrepov (v povezavi z zbiranjem, shranjevanjem ter uporabo podatkov)	***4a. Kaj menite o zakonih o zasebnosti? Ali vam dajejo občutek, da ste <u>zaščiteni</u>?*** ***4b. Ali obstajajo kakšne <u>varovalke</u> ali posebni pogoji, ki bi vas <u>pomirili</u>?***
5. Čas hranjenja nadzornih podatkov	***5a. Kaj menite o času shranjevanja nadzornih podatkov?Ali obstaja kakšna razlika?*** ***Da bi lažje raziskali, naštejte udeležencem naslednje primere:*** ***Posnetki CCTV kamer.*** ***Lokacija in gibanje vozil.*** ***Shranjevanje DNK podatkov, prstni odtisov ter posnetkov šarenice.*** ***Lokacija občanov, ki predstavljajo določeno nevarnost za druge.***

	Lokacija in gibanje starejših občanov ter otrok. ***5b. Če čas hranjenja podatkov naredi razliko, <u>koliko časa</u> naj bodo podatki shranjeni, da vam bo to <u>sprejemljivo</u>?*** *Pretečeni čas: 1 uro 35 min*
Cilji	**Povzetek razprave**
Kratek povzetek razprave [5 min] ▪ *Poudarite glavne točke razprave* ▪ *Poskrbite za dodatno priložnost za izčrpen pregled o tem, kaj je bilo povedano*	***Točka 6*** ***Na koncu fokusne skupine je koristno, da se poda nek pregled o ključnih odprtih točkah. Podajte kratko obnovo tem ter vprašanj, ki so se odprla med razpravo. Potem prosite udeležence naslednje:*** - **"Kako dobro ta obnova povzema to, kar je bilo povedano tekom fokusne skupine?"** - **"Je še kaj, kar smo pozabili povedati?"** - **"Ali smo pokrili vse?"** ***Ta kratka sekcija bo udeležencem ponudila dodatno priložnost, da izrazijo svoja stališča in se lahko uporabi tudi za pregled tem, ki so se pojavile tekom razprave, niso pa bile obravnavane med razpravo.*** ***Pretečeni čas: 1 uro 40 min***
Cilji	**Zaključek**
Zaključek fokusne skupine **[5 min]** ▪ ***Zahvalite se udeležencem*** ▪ ***Izročite povračilo stroškov*** ▪ ***Podajte informacije o projektu SMART***	***Točka 7*** **S to zadnjo vajo se je naša razprava končala. To priložnost bi izkoristil/a, da se vam še enkrat zahvalim, da ste se pridružili tej razpravi in z nami delili vaša mnenja, izkušnje ter razmišljanje.** ***Na tej točki izročite udeležencem povračilo stroškov ter jim razložite naslednje korake.*** ***Podajte več informacij o projektu SMART tistim udeležencem, ki to želijo.*** ***Pretečeni čas: 1 ura 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 Commission. 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. CCTV

1.1.1.2. Loyalty cards

1.1.1.3. Financial monitoring

1.1.1.4. Smart surveillance

1.1.1.4.1. RFID

1.1.1.4.2. CCTV with AFR

1.1.1.4.3. Gait analysis

1.1.2. Perceived purposes

1.1.2.1. Security

1.1.2.1.1. Investigation of crime

1.1.2.2. Advertising and marketing

1.2. Boundary space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. Video-surveillance

1.2.1.2. Biometric technologies

1.2.1.2.1. Fingerprinting

1.2.1.2.2. Retinal scanning

1.2.1.3. Product-detection devices

1.2.1.3.1. Luggage scanners

1.2.1.3.2. X-ray machines

1.2.1.3.3. Sensors (to detect dangerous substances)

1.2.1.4. Monitoring of personal data

1.2.1.4.1. Purchase of flight tickets

1.2.1.4.2. Passport control

1.2.1.4.3. Visa applications

1.2.1.5. Financial monitoring

1.2.1.6. Sniffer dogs

1.2.2. Perceived purposes

1.2.2.1. Passenger safety

1.2.2.2. National security

1.2.2.3. Marketing purposes

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. Video-surveillance

1.3.1.2. Law enforcement personnel and security officers

1.3.2. Perceived purposes

1.3.2.1. Public security
1.3.2.2. Citizen safety
1.3.2.3. Crime prevention and investigation
1.3.2.3.1. Crowd monitoring and control
1.3.2.3.2. Timely identification of known or suspected hooligans
1.4. Mobile devices and virtual spaces
1.4.1. Awareness of different surveillance methods/technologies
1.4.1.1. Location tracking via GPS
1.4.1.2. Monitoring of call and message lists
1.4.1.3. Recording of conversations
1.4.1.4. Data collection & sharing through smart phone applications
1.4.2. Perceived purposes
1.4.2.1. Security-related purposes
1.4.2.2. Commercial reasons

2. Perceptions and attitudes towards smart surveillance and integrated dataveillance
2.1. Feelings
2.1.1. Disbelief
2.1.2. Extreme discomfort
2.1.2.1. Horror
2.1.2.2. Uncomfortable
2.1.3. Convenience
2.2. Behavioural intentions
2.2.1. Active reactions
2.2.1.1. Questioned the civil servant
2.2.2. Passive reactions
2.2.2.1. Cut off all communication
2.3. Beliefs
2.3.1. Likelihood of massively integrated dataveillance
2.3.1.1. Technical aspect
2.3.1.1.1. Possible
2.3.1.1.2. Occurring in a covert manner
2.3.1.2. Technical aspect
2.3.1.2.1. Currently illegal
2.3.1.3. Ethical aspect
2.3.1.3.1. Unacceptable
2.3.2. Acceptance of massively integrated dataveillance
2.3.2.1. Acceptance contingent on different factors
2.3.2.1.1. Purpose of data collection
2.3.2.1.2. Type of data
2.3.2.1.3. State vs. private enterprises

2.3.2.2. Unacceptable due to different factors
2.3.2.2.1. Risk of misuse
2.3.2.2.2. Fear of discrimination
2.3.2.2.3. Possible tool to exert control and power
2.3.2.3. Benefits of data collection
2.3.2.3.1. Statistical analysis
2.3.2.3.2. Provision of free services
2.3.2.3.3. Enhancement of service efficiency
2.3.2.3.4. User convenience
2.3.2.4. Self-responsibility of citizen
2.3.3. Perceived privacy impact of smart technologies
2.3.4. Perceived effectiveness of smart technologies
2.3.4.1. Decision-making capabilities of automated systems
2.3.4.1.1. Advantages of automated systems
2.3.4.1.1.1. Machines more objective
2.3.4.1.1.2. Subjectivity of human agency
2.3.4.1.2. Disadvantages of automated systems
2.3.4.1.2.1. Possibility of misinterpretations or wrong conclusions by machines
2.3.4.1.2.2. No possibility of negotiation with a machine

3. Security-privacy trade-offs

3.1. Acceptance of technological surveillance
3.1.1. Feelings
3.1.1.1. Insecurity
3.1.1.2. Safety
3.1.2. Beliefs
3.1.2.1. Controlling function of surveillance
3.1.2.1.1. Violation of privacy
3.1.2.1.2. Instrument to suppress and control
3.1.2.1.3. Criminalisation of citizens
3.1.2.1.4. Threat of data misappropriation and misuse
3.1.2.2. Caring function of surveillance
3.1.2.2.1. Increased security
3.1.2.3. Effectiveness of surveillance
3.1.2.3.1. Useful in terms of investigation
3.1.2.3.2. Futile in terms of prevention
3.1.2.3.3. ‘False’ solution
3.2. Perceptions of different technologies
3.2.1. Vide-surveillance
3.2.1.1. Acceptable in public places
3.2.1.2. Unacceptable in private spaces

3.2.2. Biometric data

3.2.2.1. Invasive

3.2.2.2. Acceptable specifically for forensic purposes

3.2.3. Electronic tagging (RFID)

3.2.3.1. Extremely invasive

4. Surveillance laws and regulations

4.1. Feelings and beliefs

4.1.1. Lack of information

4.1.1.1. Lack of initiatives at raising awareness

4.1.1.2. No interest by citizens

4.1.2. Perceived effectiveness of the legislation

4.1.2.1. Trust in the legislation

4.1.2.2. Legislation can never be fool proof

4.1.2.3. Effectiveness depends on enforcement

4.1.3. Suggested safeguards

4.1.3.1. Informing citizens about data sharing

4.1.4. Length of data storage

4.1.4.1. Short storage periods

4.1.4.2. Longer duration for biometric data