SMART

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

Noellie Brockdorff[1], Natalie Mundle[1], Christine Garzia[1], Walter Hoetzendorfer[2]

[1] Department of Cognitive Science, University of Malta, Msida, Malta

[2] Centre for Computers and Law, Universität Wien, Wien, Austria

December 2013

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

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

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

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

Table of Contents

Appendices

1. Key Findings

This document presents the Austrian 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 19 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 focus group 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 Austrian participants were overall highly aware of the deployment and purpose of surveillance measures in different contexts. The findings indicate that surveillance in commercial, boundary and public spaces has undergone a process of normalisation. In these spaces, technological surveillance was deemed predominantly acceptable for different reasons, including marketing and security-related purposes. Another context discussed was the virtual space and although the participants' showed a general awareness of the surveillance methods used in this context, it appears that they were unsure of which type of data is exactly being collected and by whom.

In order to gauge participants' attitudes and beliefs on dataveillance, the group was presented with a fictional scenario illustrating the massive integration of data. After an initial intense reaction to this situation, the participants debated the possibility of dataveillance and massive integration of personal data taking place and proceeded to differentiate between technical, ethical and legal aspects. Although a development in this direction was regarded as realistic from a technological viewpoint, the actual probability of massively integrated dataveillance occurring was considered as low since the participants not only perceived this as unlawful but also as unethical.

Different types of surveillance measures and technologies, including CCTV systems, biometric technologies and electronic tagging, appeared to meet varying levels of acceptance. Participants generally displayed a positive attitude regarding the use of CCTV in commercial, boundary and public spaces, which appears to result from the perception that CCTV enhances security for both citizens and society at large. In terms of the effect of such systems on citizens, whilst some participants felt that the use of video-surveillance has a negative effect on individuals, the majority of participants perceived a minimal effect on citizens' privacy, especially when video surveillance was of an inconspicuous nature. It appears that the visibility of such systems was perceived by some participants as drawing attention towards the possibility of danger, thus contributing to feelings of insecurity rather than safety.

In relation to surveillance involving the physical sphere, in particular biometric technologies and electronic tagging, most participants considered such methods as extremely intrusive, not solely from a privacy aspect but also in relation to the free movement of citizens. Participants additionally perceived that the use of such physically invasive surveillance may lead to a sense of dehumanisation. Moreover, in addition to presenting a threat to privacy and freedom, some participants argued that such an intensification of surveillance would also result in a general criminalisation of citizens.

Beliefs and opinions on the effectiveness of surveillance from a security aspect were rather mixed, both in relation to the autonomous decision-making capabilities of smart technologies as well as to the overall effectiveness of surveillance. In relation to the first aspect, some participants perceived the automatic decision-making process as being devoid of biases and subjectivity and thus as more objective than human decision-making. Moreover, participants perceived smart surveillance as affording a faster reaction time to events. On the other hand, other participants expressed mistrust of technologies operating without any human supervision, perceiving the possibility of wrong decisions being taken by the system.

In relation to the overall effectiveness of surveillance, while some participants expressed their confidence in the ability of surveillance measures to combat crime and thus provide protection to citizens, others were more sceptical. These participants argued that surveillance served to satisfy society's need to feel secure instead of being effective in deterring criminals and reducing delinquency. A main reason that surveillance was deemed as ineffective was the belief that criminals would manage to circumvent surveillance.

Participants were also invited to share their viewpoints on surveillance laws and regulations. Although they claimed that general information about laws is insufficient, it appears that the majority have a solid trust in national legislators and in current legislation. This notwithstanding, a better protection of personal data by the Data Protection Commissioner was called for. In addition to a lack of information about the law, participants also criticised the lack of information available about the surveillance measures which have been implemented nation-wide and are currently in use. Furthermore, another main criticism was that current laws were outdated due to the fast advancement of technology.

2. Introduction

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

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

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

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

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

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

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Overall, 353 participants took part in this research project. All 42 groups had between 6 and 10 participants, excluding 3 groups which had 11, 12 and 13 participants respectively. The focus groups in Austria were carried out on the 12th March, 2013; 20th March, 2013 and 24th April, 2013[2]. The composition of the groups held in Austria 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

[2] The first two groups were conducted prior to the Boston Marathon bombings whilst the last one was carried out after. Participants in FG III mentioned terrorist attacks, including the Boston bombings a few times, and had a short discussion about surveillance in relation to terrorist attacks; however, there was no significant difference in the attitudes of participants in this group and those of participants in the other two groups.

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

The discussion guidelines were translated into each national language where the research was conducted. Moreover, back translations were carried out which entailed an independent translation of the discussion guidelines back into English by a different translator. The back translation was then compared with the original version in order to ensure comparability of meaning and clarify any possible discrepancies. Any possible changes were discussed with the partners, and, where relevant, the necessary amendments were carried out until a final version of the discussion guidelines in the national language was approved. The Italian 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 Austria is based on a total of 19 participants since a number of participants, most notably in Group 1 (18-24 years), did not show up on the day. Moreover, it was noted that it proved rather difficult to find participants willing to attend the focus groups; this was particularly the case for Group 3 participants (45+ years).

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	F	M	F
P2	M	F	M
P3	F	M	M
P4	M	F	M
P5	F	F	F
P6	F	F	M
P7	-	M	-
Total	**6**	**7**	**6**

Although there were slight differences in the atmosphere of the three groups, in general the atmosphere was described by the moderators as friendly, open and agreeable. The discussion was described as generally smooth and free-flowing, with the exception of Group 3 (45+ years). Additionally, the discussion in Group 1 (18-24 years) was described as being rather intense and engaging, while the discussion in Group 2 (25-44 years) was more balanced and the participants tried to seek a common position. Lastly, it appears that one of the participants (P6) in Group 3 (45+ years) was considered as adopting a controversial stance specifically in relation to privacy rights' most probably due to his role as an entrepreneur.

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, in this case supermarkets, a number of surveillance technologies and methods, including CCTV and loyalty cards, were mentioned by participants. In general, it appears that CCTV has been widely accepted as a standard surveillance tool in supermarkets. Various purposes of surveillance by CCTV were mentioned; the majority of the participants perceived the observance of customer behaviour for security reasons and marketing purposes as a predominant objective.

In addition, the use of loyalty cards in supermarkets and their purpose was perceived as evident: "*Certainly they use loyalty cards to collect data. This is their purpose*" (P1-I). The collection of customer data through loyalty cards was perceived as a method for commercial enterprises to customise advertisements, offers and emails, which the majority of focus group I members (18-24 years) regarded as advantageous for customers. Most participants appeared to value the benefits provided through bonuses and product discounts. To a lesser degree, focus group II (25-44 years) members added an enhanced shelf, product and personnel organization as further advantages of the use of CCTV and loyalty cards.

On the other hand, participants were also clearly aware of the other side of the coin linked to the possible sharing of personal data, in particular payment details, and the likelihood of data misuse. However, it appears that the sharing of personal data with commercial entities was, in the case of loyalty cards, deemed as acceptable since this was ultimately considered as a choice, whereby "*every single mature customer*" (P2-III) has the possibility to refuse or accept the sharing of their personal data.

5.1.2 Boundary Space

In the context of border control, the discussion mainly focused on an airport setting as a boundary space, while, to a much less extent, surveillance at land borders was also briefly discussed. At the outset, some participants, particularly those in Group I (18-24 years), argued that surveillance in the context of air travel is already underway prior to physically entering the airport: *"[…] you are already monitored when you book the flight"* (P4-I). In this context, participants perceived national security as being the predominant purpose of surveillance. In all groups, the airport was considered as a space where surveillance is ubiquitous: *"Every corner is illuminated"* (P6-III). This perception was especially due to the extensive use of CCTV: "*Every step is surveilled there*" (P4-I). In line with the pervasiveness of surveillance in this space, a variety of technologies and methods utilised for surveillance was mentioned by the different groups. In addition to CCTV, participants mentioned a number of object and product detection devices, such as luggage controls, full body scanners as well as knife and drug detectors. Passport and criminal record checks were also regarded as main sources of surveillance. Additionally, members of focus group II (25-44 years) also discussed the use of biometric technologies, including fingerprinting and facial recognition. In certain instances, it appears that biometric surveillance elicited a sense of discomfort; as recalled by a participant who had to provide his fingerprints upon arrival to the United States: "*That would have been a reason for me not to visit the U.S., but in the end I did*" (P5-II).

It seems that some participants perceived a number of differences between surveillance measures in Austria and in other countries. Firstly, it seems that participants perceived national surveillance measures in Austria as being *"lax"* (P1-II) and *"not that strict"* (P4-II) in comparison to other European countries. Some also held the belief that citizens in other countries are more concerned with security issues: "*In the UK it is hardcore. If you go away just one meter from your luggage, about 50 people come and freak out*" (P7-II). Moreover, it appears that some participants perceived certain surveillance methods, such as facial recognition, as being more commonplace in other countries, especially in countries outside of Europe.

Although in general participants perceived the escalating use of surveillance measures in this space as being justified, at the same time some expressed concern that the acceptance of new technologies thrives on fear and vulnerability regarding potential risks: "*There are a lot of technologies, which are not yet in use. They just wait until something bigger happens to enforce safety measures, which are not that tolerated by the population*" (P7-II).

5.1.3 Common Public Spaces

In common public places, such as stadiums where mass events are organised, CCTV was perceived as the predominant surveillance technology used by police and security officers mainly for safety and security-related reasons. More specifically, the use of video surveillance was regarded as a tool for crowd monitoring, for the regulation of visitor flows and for the facilitation of evacuation processes in case of emergency. To a lesser degree, participants also mentioned the use of object detection devices as a security measure.

In addition, the monitoring of personal information for security-reasons was also discussed in this context; here the focus group participants mentioned the process of identity checks upon entrance to a stadium: *"you cannot simply go there as an anonymous person*" (P4-I). Some participants also drew attention to the monitoring which takes place through the personalisation of tickets. It appears that one of the perceived reasons for these identity checks is to decline entry to individuals who are identified as being banned from attending such events.

The use of surveillance in other public spaces such as museums was also discussed. Participants mentioned CCTV systems as being useful for the protection of property and artefacts, for the prevention of theft and also for crime investigation. The collection of personal data was also discussed in this context; participants perceived the gathering of data as having a certain utility for the organisation in relation to statistical purposes, marketing reasons and resource management. In general, it appears that participants perceived the aforementioned surveillance measures in the public space as justified, and hence as acceptable.

5.1.4 Mobile Devices and Virtual Spaces

Participants mentioned a variety of ways surveillance occurs through the use of mobile telecommunication devices, including the recording of conversations, GPS tracking and the collection of data through smart phone applications. In general, the perceived purposes differed according to the type of data gathered. The recording of conversations and GPS tracking were both regarded as having a preventive and necessary function in the context of crime, including the ability to trace criminals. Additionally, the GPS tracking of mobile phones was also perceived as being utilised by private companies in order to collect data for commercial purposes. Such use was perceived as unacceptable and in fact the participants described how when knowledge of this came to light, it caused a national scandal. Along similar lines, the participants argued how the profitable business of selling customers' data poses a major threat to citizens. Here, the participants expressed their uncertainty and anxiety not only in relation to the storage of their personal data: *"I do not know where my data ends up"* (P5-I) but also on the use of such data *"[…] how the data is used afterwards, nobody knows"* (P3-I).

Significantly fewer participants mentioned the collection of data through smart phone applications. It seems that these participants were suspicious of these applications since their origin is almost impossible to trace. In turn, this lack of knowledge led to a sense of insecurity vis-à-vis which privacy and data protection laws would take effect if a foreign company owned the application:

> "*I do not know where my data ends up, at which companies it ends up and which companies on the other hand are involved. I cannot trace the purpose any more … and there are large security gaps in programs, especially in small Apps*" *(P5-II).*

With particular reference to virtual spaces, although participants appreciated the legal protection of personal data, they acknowledged their own role in divulging personal information online, especially via social networks: "*We feed information into the system on our own*" (PII-1). In this space, they appeared to be aware of their data being used for marketing purposes by noticing an increase in customised advertisements. In relation to potential risks in the virtual space, focus group III (45+ years) participants seemed particularly concerned about divulging financial details online.

Overall, albeit the participants' showed a general awareness of the surveillance methods used in this context, it appears that they were unsure of which type of data is exactly being collected and by whom.

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 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 tap into the attitudes of the participants, the group was presented with an everyday scenario: a recorded telephone conversation between a job seeker and a civil servant of the employment agency, where complex surveillance[4] becomes evident.

5.2.1 Feelings

After having listened to this conversation, the focus group participants revealed feelings which predominantly indicated an extreme sense of discomfort: likened to "*George Orwell's 1984*[5]" (P5-III), this *"scary"* (P5-I) scenario gave rise to a range of feelings which included feeling *"very uneasy"* (P6-II), *"surprised"* (P5-I) and *"insecure"* (P2-I). It appears that such feelings stemmed from the perception of being "*pursued and examined, in every respect*" (P6-II). In fact, this extreme discomfort was also at times described in physical terms, whereby for instance one participant stated he would feel *"naked"* (P4-I) in such a situation.

In addition to such discomfort, other participants also appeared to experience a sense of helplessness and resignation, comparing the situation to an inevitable trap: "*You cannot escape it*" (PI-1). Additionally, other participants perceived themselves as being victims of manipulation, stating that they would feel "*properly fooled*" (P5-II). Lastly, it appears that only a minority of participants, particularly those in focus group II (25-44 years) and focus group III (45+ years), experienced indignation at such a perceived violation of privacy: *"I would feel deeply insulted"* (P2-III). Lastly, one participant expressed his intention of possibly building up a network of consumers, similar to a group like Anonymous[6], in order to oppose the surveillance procedures of the state and the selling of data by commercial *"global players"* (P5-I).

5.2.2 Behavioural Intentions

In addition to asking about their feelings upon listening to this conversation, participants were also asked for their resulting behavioural intentions. While some participants suggested a rather passive reaction involving some kind of immediate withdrawal from the hypothetical situation, such as hanging up the

[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. See Appendix B, Item 4 for full text of scenario.

[5]The author George Orwell published the book "Nineteen Eighty-Four" in 1949, which describes a dystopian vision in which government surveillance is omnipresent.

[6]Anonymous is a network of hackers and activists which became known for carrying out cyber-attacks on governmental and corporate websites which they accused of censorship.

phone, the majority of participants claimed they would engage in a variety of behaviours in order to counteract such a situation. Mainly, these behaviours included self-protection strategies and pursuing legal action.

In relation to self-protection strategies, participants mentioned a number of behaviours they could possibly engage in. These participants stated that they would try to *"fool the system"* (P5-II) via a number of actions, in particular those relating to online behaviour. Specifically, participants declared they would be *"careful"* (P3-I) when it comes to sharing personal data, especially in cases of online purchases: *"I would stop buying books online and would not book flights by credit card"* (P2-II). Additionally, albeit participants seem to have focused more on online behaviour, some also mentioned possible actions in the 'physical world': *"I would wear a wig and change my walk"* (P2-II). In general, while such behaviours appear to suggest that these participants believe in their own ability to protect themselves from unwanted surveillance measures, the participants at the same time questioned whether such attempts at self-protection would in practice be effective.

Additionally, other participants declared that they would resort to legal action, such as filing a complaint with the Data Protection Commission. Such strategies seem to suggest a certain faith in the existing legal system and protection by law. Some participants also mentioned that such a situation would have a significant bearing on their vote: "*I would refuse that the constitutional state develops in that direction. In this case as a citizen I would think twice how to decide at the elections*" (P5-III).

5.2.3 Beliefs

5.2.3.1 Likelihood of smart surveillance and integrated dataveillance

Regarding the likelihood of whether or not smart surveillance and massively integrated dataveillance are possible (currently and/or in the future), the focus group participants generally distinguished between technical, legal, and ethical aspects. Generally, the development of massively integrated dataveillance was perceived to be "*indeed possible*" (P4-II) from a technical aspect, however, not to the extent as portrayed in the scenario, mostly due to the state of current legislation as well as due to ethical considerations.

From a technical viewpoint, although the scenario was perceived as being rather *"exaggerated"* (P4-II), most of the participants believed that this is in practice possible since they argued that *"the data is already available, what is missing is just its integration*" (P3-III). Nevertheless, one participant pointed out that intrusive surveillance is not a recent phenomenon but one which already existed decades ago, even without the presently available smart methods and technologies:

> *"[…] the security service during the Nazi era had millions of informers, who particularly spied on the everyday behavior of people. This was condensed then passed through the hierarchy and up there they drew conclusions accordingly […] of course not by the means we have today" (P2-III).*

Whilst such data integration was deemed as *"unlawful"* (P3-III) due to the limits imposed by existent legislation, some participants did not exclude the possibility that this kind of intrusive surveillance and dataveillance would become legal in the future since *"the trend is going in that direction"* (P6-II). Nevertheless, some participants argued that the spread and intensification of surveillance technologies and methods is not merely a technical or legal issue. These participants argued that the likelihood of such surveillance is unlikely since it is *"unacceptable"* (P1-II) from an ethical standpoint. For some participants, the notion of freedom was perceived as being more valuable than security: *"[…] somewhere you have to draw the line. Personal liberty rights are worth much more and the line moves slowly and subtly, but I think that for most people the line lies quite high*" (P1-II).

Nevertheless, while in general the participants perceived this scenario as unacceptable, there was a minority of participants who did not strictly object to it. While in part it appears that such acceptance resulted from a strong trust in *"legislators"* (P6-III), acceptance of surveillance was also contingent on whether *"the political system is ok"* (P6-III), most probably alluding to a democratic political system.

5.2.3.2 Perceived effectiveness of smart technologies and dataveillance

Issues of effectiveness were also brought up by the participants and effectiveness was discussed from different perspectives. In essence, the participants debated the *"double-edged"* (P6-II) nature of surveillance, underscoring a variety of perceived advantages and disadvantages pertaining to smart technologies and the massive integration of data from dataveillance.

Some participants stated their belief that the sharing of data can be convenient and practical in certain cases, such as the sharing of medical data. Nevertheless, others drew attention to the inherent risks pertaining to data sharing: *"I think that it is basically a good idea. But one has to guarantee that only the persons concerned have access to the system. This is difficult"* (P1-II). In addition, another aspect mentioned by the participants was that smart technologies enable the analysis of vast amounts of data, which otherwise would not be possible.

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 *"machines"* (P4-I). In this regard, a number of participants perceived automated systems as being more *"objective"* (P4-I) since there is no human agency involved. These participants argued that, in contrast to machines, humans are influenced by their biases, an aspect which introduces an element of subjectivity in decision-making: "*[…] the person, however, has feelings too. The machine just triggers the alarm when a behavioural pattern occurs. The person presses the alarm button when someone has the 'wrong' skin colour*" (P7-II). However, this viewpoint was challenged by some participants who argued that *"the machine is programmed by the human. The human who is programming it will put his visions into the machine […] you cannot separate these things*" (P5-II). 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, some participants appeared to be skeptical and distrustful of technology on its own without human agency. These participants appeared to challenge the decision-making capabilities of smart technologies, and seemed particularly concerned about the likelihood of ‘wrong’ decisions by automated systems:

> *“I think that if there are mistakes through this smart interlinking of data and wrong conclusions are drawn, they can then be used against me in some way. Then I have to prove [my innocence] and give evidence against that” (P1-III).*

Another aspect discussed in relation to effectiveness was the perception that, due to its automated nature, smart surveillance enables a faster reaction time to events in contrast to traditional surveillance technologies. For instance, smart CCTV systems were considered as providing the possibility to *“react more quickly in certain situations and prevent things, perhaps”* (P5-I) as opposed to traditional CCTV: *“it is obvious that it doesn’t help immediately”* (P3-I). As argued by another respondent:

> *“I think that, referring to video surveillance, this [smart CCTV] would be more effective, because video surveillance as it is now does not always work, I think. You don’t feel safe because in the subway there is a camera somewhere. This has, I think, little effect. If a camera is hanging there which monitors me, then one which alerts when something happens is probably more effective than one which is just there” (P1-I).*

Therefore, albeit some participants perceived cameras as having a *“deterrent effect”* (P5-III), it seems that a number of participants did not consider traditional CCTV systems as being effective since they believed that human operators would not be watching the screens in real time; thus, *“if something happens there, then you can just hope that someone passes*” (PI-4). In light of this, certain participants indicated that they would prefer an increased presence of security personnel or police officers.

5.3 Security-Privacy Trade-offs

5.3.1 Acceptance of Technological Surveillance

In order to gauge participants' perceptions vis-à-vis the security-privacy trade off, as well as their attitudes towards a number of specific smart technologies, a hypothetical scenario was presented to the group. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging. The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[7].

When discussing the scenario, a number of participants had a very intense reaction, perceiving this *"depressing"* (P1-I) scenario not only as extreme: "*This clearly goes too far*" (P6-I) but also as unnecessary given that in past times, even without the use of such technology, *"crimes were still solved"* (P1-II). Rather than enhancing feelings of personal safety, the security measures portrayed in the scenario resulted in feelings of insecurity amongst some participants: "*I would definitely feel considerably more unsafe"* (P1-I). Several participants from the different age groups also revealed an increased sense of vulnerability: *"This opens the door to a different kind of crime, this is very worrying"* (P1-I).

A number of reasons can be attributed to this increased sense of insecurity and vulnerability. Some participants explained this by describing how the presence of certain surveillance measures, in particular overt measures such as cameras, heightens their awareness to the possibility of danger. Thus it appears that the visibility of surveillance measures might contribute to feelings of insecurity:

> *"I am really sensitive with cameras and I don´t feel safer in the metro just because there is a camera, quite the contrary, I think there must be a reason why there is a camera. I don't feel this emotional security as some people do" (P2-II).*

Additionally, this vulnerability seemed to stem from the increased possibility of data misuse: "*With these means it is presumably easier [to solve crimes]. But on the other hand, if these data fall into the wrong hands then […] you never know who will, in the end, be in charge of that"* (P6-I). It seems that the majority of participants perceived the misappropriation and misuse of personal data collected by smart surveillance and dataveillance as a very realistic and major threat: "*On the internet as well as in real world, you just need the means and the interest for it"* (P5-II).

Moreover, a number of respondents expressed concern at the way that surveillance measures affected their privacy, further arguing that their acceptance of surveillance procedures was contingent on the

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

extent that such measures impinged on their privacy. While for these respondents privacy was considered as more important than security, there were participants who in addition revealed other concerns besides privacy reasons. Ethical issues pertaining to *"freedom"* (P2-I) and *"control"* (P1-I) were underscored by these respondents: *"[this] does not have any humanity anymore"* (P2-I) and once again they revealed a great sense of vulnerability: "*This is control and not protection"* (P1-I). In fact, some associated this type of intrusive surveillance with a communist political system:

> *"I think this does not have anything to do with security any more. The headline to this could also be "communism is back again". It is similar to twenty or thirty years back in the East [with the difference that] new technology is used to do it" (P3-I).*

In particular, the respondents appeared concerned that the focus of surveillance could shift from monitoring criminals to observing all citizens. They argued that such an intensification of surveillance would not only represent a threat to privacy and freedom but also result in a general criminalisation of citizens:

> *"Once implemented, who can tell whether these measures will be quickly abolished […] and then this turns into another direction, that you are guilty before anything is proven, only because the camera sends off an alarm*" *(P6-1)*

Another issue discussed during the focus groups was the effectiveness of surveillance measures in combating crime and thus in providing protection to citizens. In general, it appears that perceived effectiveness had an influence on acceptability of surveillance measures. Beliefs and opinions in this regard were rather mixed. To start with, it appears that some participants justified surveillance due to the belief that, although at a cost, it provides stability and order to society:

> "*Primarily the surveillance is here to help and to protect us and it is obvious that there is always a good and a bad side. You have to expect that. If there was no surveillance, anarchy would reign and we would have to be much more afraid. We have to take this into consideration" (P3-I).*

Similarly, other participants expressed their confidence in surveillance measures: "*If surveillance measures lead to a higher crime clearance rate, then more potential criminals are kept away from the public, they are jailed for some time. This alone could already make a difference*" (P5-III). Nevertheless, while these participants revealed their appreciation for the caring function of surveillance, other respondents showed a more cynical attitude. Firstly, some participants underscored the issue of proportionality in relation to the large numbers of citizens being monitored and the amount of criminal cases solved through the use of surveillance: *"Why should I subject 5 million passengers to something in order to catch two or three pickpockets?"* (P2-III) Secondly, other respondents challenged the notion that surveillance can, in and of itself, guarantee security: "*I don´t think that surveillance is effective. You have to fight the root of crime, because surveillance provides no challenge*" (P5-II). Rather, these participants believed that only the subjective feeling of security was actually satisfied in society. A number of participants argued that the introduction of surveillance measures thrives on scaremongering tactics: *"I think that in a lot of countries people are manipulated, that you have to do it that way. But in fact it does not change anything about the problems"* (P2-II). Such an argument touches on the political side of surveillance, and some participants argued that surveillance is a profitable business for different factions: *"I think money is involved. The politicians realize that they get a lot of power with fear, like in the U.S. and the companies benefit"* (P2-III). Some participants felt that citizens are led to believe that the crime rate is higher than it actually is since this was perceived to promote the acceptance, and tolerance, of surveillance in society.

Surveillance measures were also deemed as ineffective due to the belief that wrongdoers would somehow still manage to "*circumvent everything"* (P3-I) through a variety of ways and means: "*Because the criminals know how to protect themselves, they know how to paint their fingerprint with a special layer, how to use contact lenses, how to change their walk not to get caught"* (P5-II).

5.3.2 Perception of Different Technologies

In general, different types of surveillance technologies seemed to meet different levels of acceptance. Firstly, although video surveillance was generally considered as acceptable, a number of participants did express their reservations in relation to CCTV, especially smart CCTV. ANPR was also deemed as acceptable, especially since this surveillance technology was perceived as a useful tool for locating stolen vehicles. On the other hand, the use of biometric data and electronic tagging were, in most cases, considered as not acceptable.

In relation to CCTV, some participants perceived the acceptance of this technology as possibly resulting from the normalization of surveillance: *"Video surveillance has been in existence for a long time; we are used to it. In every subway station, in every square, they are installed. Maybe there is already an effect of habituation*" (P1-III). Overall, these participants perceived CCTV systems as an appropriate security measure and claimed that it was neither affecting their privacy nor resulting in any change of behaviour. In addition, other participants underscored that their reactions to video surveillance was contingent on the extent of visibility: *"The thing is that the cameras that we see affect us, but I'm not affected by those I don't see. The feeling of being monitored vanishes if you don't see it directly. It is a rather subjective feeling" (P5-III).*

In relation to the above, several participants revealed that without the use of signage indicating the presence of CCTV systems, they would feel more at ease since they would 'ignore' the cameras. However, in contrast, others stated that they would appreciate being informed of the presence of CCTV systems since such information would give them the opportunity to adapt their behaviour accordingly. Additionally, a minority of participants said that without any signage, they would make an effort to find out where a camera could possibly be located.

As mentioned above, some respondents objected to the use of CCTV systems. These participants, mainly from Group II (25-44 years), perceived cameras as potentially having a negative effect on both their feelings and their behaviour: *"If you know that you are surveilled, then you behave differently. Then you think twice before saying something and you are more self-conscious, not so natural"* (P6-I). Some stated that whilst the presence of CCTV did increase their feelings of safety, at the same time the cameras made them feel *"annoyed"* (P7-II) and *"queasy"* (P5-II). As stated by one of the respondents:

> *"The cameras for sure contribute to feeling safer and in the metro I would definitely feel safer, but the cameras should not be everywhere. This would make me feel very restricted in my behavior. I would at some point behave a little bit differently on the street" (P4-II).*

In particular, there were respondents who considered smart CCTV as *"a huge intrusion"* (P1-I). Automatic face recognition was perceived rather negatively by these participants, who considered this function as *"limiting"* and *"frightening"* (P1-II). Nevertheless, when it came to contexts which are generally considered as sensitive, such as airports, the participants indicated their acceptance of face recognition devices.

The use of electronic tagging and biometric data – hence surveillance involving the physical sphere – was in general considered as extremely intrusive: *"I don´t want to give away anything which has to do with my body, not even to a country; neither my finger print or my hair, nor my DNA* (P5-II). In general, the collection of this type of data was perceived as presenting a higher threat to privacy:

> *"I think it is ok that nowadays there are cameras in public spaces but electronic tags on every person and DNA and fingerprints, I wouldn't want to give that away. As an innocent I would feel forced to give away my most private things" (P2-I).*

Participants seemed to convey a heightened sense of vulnerability in relation to biometric surveillance and, in particular, some respondents expressed concern that the use of biometric systems could result in identity theft. Additionally, while the tracking of people via electronic tagging was overall perceived as impinging on the free movement of individuals, it was considered as "*always a good thing*" (2-II) in cases of emergency such as the tracking of missing persons.

With regards to locations of deployment, surveillance was considered as generally acceptable in public places, such as city centers and educational institutions, as well as private commercial establishments such as shopping centers and hotels. Moreover, participants also indicated their acceptance of surveillance in places considered as high risk areas, such as airports. It appears that in general, surveillance in public places was considered as part of the 'caring' function of surveillance. On the other hand, surveillance was considered as unacceptable in private spaces such as one's home and other places where people seek to unwind: *"In public I find that all right, too. In a park I don't want to have these surveillance cameras, but perhaps it is ok because of pickpockets, but not when I am at my friend's place"* (P2-I).

5.4 Surveillance Laws & Regulations

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

5.4.1 A lack of information and transparency

The first issue under discussion was the accessibility and transparency of surveillance laws and regulations. The focus group participants, in particular those from Group II (25-44 years), argued that access to general information was insufficient and certain participants revealed a sense of helplessness due to the steadfast advancement of technology: "*The information is slower than the technology. What we wish, that we learn more about it, how to protect ourselves, will always be insufficient*" (P2-II). In particular, the respondents argued that there is a lack of information in relation to which surveillance measures have been implemented nation-wide and are currently in use. As stated by one participant, there is a lack of transparency in this regard:

> *"[...] it is hardly comprehensible. The biggest disadvantage to me is this lack of transparency. But I don´t want to resign and to stop being critical just because it is hardly comprehensible […] you need hundreds of sources of information and you are on your own" (P5-II).*

In general, these participants pointed out that they felt under-informed as 'normal' citizens about their privacy rights, and that this lack of knowledge was perceived as hampering protection measures and legal actions against any abuse of surveillance. Nevertheless, some participants acknowledged the lack of initiative by citizens in getting informed as being part of the problem.

5.4.2 Effectiveness of laws and regulations

Another issue discussed was the effectiveness of privacy laws. Firstly, some participants argued that the rate at which technology develops is so rapid that changes in legislation just *"cannot keep up"* (P5-II). Focus group participants, in particular those in Group II (25-44 years) argued that the state is, from a legal viewpoint, always one step behind the developments of the fast-moving technological market: "*the progress is faster than the legislation*" (P7-II). This was perceived as especially pertinent to highly advanced surveillance technologies: "*Technologies which we probably just know from James Bond will quickly become reality and legislation will always be too late*" (P2-II). Thus, current laws were perceived by the participants as being outdated in this regard. In contrast to the above, one participant perceived privacy laws and general data protection measures as being extremely restrictive. From an entrepreneur's viewpoint, this participant expressed his dissatisfaction about the legislator transferring too many rights to data protection activists "*Data protection activists have fifteen times the power they* *should have in this state*" (P6-III). This participant thus perceived the current legal situation as disadvantageous for his business as well as for the national economy.

Another issue discussed relating to effectiveness was that of data protection in the virtual space. Some participants argued that not only would it be problematic to trace the possible use or misuse of data, but that difficulty would also arise in relation to which legislation, either national or international, would take effect in cases of misuse. These concerns led to a sense of vulnerability amongst some participants: "*If someone wants to do you harm, you don't stand a chance on the web*" (P4-III). Thus, these participants stated that the current legislation needs to be revised in order to take these aspects into consideration. Similarly, other participants pointed out that the legal situation on the internet was evidently not transparent enough and argued that in case of difficulty, it was unclear how to proceed and what action can actually be taken: "*It is like you have no rights at all*" (P5-II).

5.4.3 Level of trust in the state

Some participants expressed a certain lack of trust in the protective measures of the state. This mistrust appears to have resulted from the occurrence of a series of data protection scandals as well as perceived issues of injustice pertaining to the tax administration system. For these participants, the state was perceived as having ulterior motives vis-à-vis the collection and analysis of surveillance data:

> *"[…] But if at least the state and the authorities could guarantee that it [surveillance data] is used to the benefit of the citizens then it would be good. But it´s not like this. The benefit for yourself is a different one than the one for the state" (P4-II).*

Some participants criticised the Data Protection Commissioner for the perceived lack of action in cases of data sharing and data selling between private companies, an issue which is discussed in more depth below. Nevertheless, regardless of the mistrust and dissatisfaction delineated above, it appears that the majority of the participants have a solid trust in national legislators and legislation:

> "*I think the data protection law achieves high standards in Austria. It is in the nature of things that there is no 100% protection. Probably the law could be improved, but the existing structure is a good protective mechanism*" (P1-II).

5.4.4 Level of trust in private actors

Regarding the level of trust in private actors, while it appears that the participants perceived that they could trust most local companies, the misuse of data appeared to represent a realistic threat for the participants. The participants argued that private companies could easily circumvent current surveillance legislation and in addition some participants expressed their doubts regarding the likelihood of new legislation setting more restrictions to data sharing. In their opinion, *"the lobby behind them is too strong"* (P6-I).

5.4.5 Length of data storage

Participants were also asked about their opinions on the length of storage for surveillance data. In general, participants of focus group I (18-24 years) and II (25-45 years) argued that storage time should ideally be between six months and one year. The purpose of data collection was considered to be an important criterion for the appropriateness of the length of storage. Nevertheless, in cases of crime investigation, the majority of participants agreed upon a longer time frame, with some even agreeing to an indefinite storage time. Additionally, the type of surveillance data was also considered to be important. However, in this case, the participants of these two groups expressed different and partly contradictory opinions, ranging from the immediate deletion of number plate recordings to an indefinite storage of biometric data.

In contrast to the other respondents, focus group III members (45+ years) believed that storage limits should be removed, mainly due to the belief that they present a source of hindrance for crime investigations such as tax evasion. However, at the same time, the participants did acknowledge the technical limits involved in retaining data indefinitely.

5.4.6 Data sharing between different actors

Overall, it appears that the acceptance of data sharing between different actors was contingent on a number of factors, primarily on whether consent is given by the individual as well as the type of information to be shared. Generally, participants considered the sharing of data acceptable as long as the personal data was provided by the individual on a voluntary basis and consent was expressly given for data sharing. With regards to the type of data shared, the sharing of health and medical data appeared to be a rather sensitive issue. While the sharing of such data between doctors was in general considered as acceptable, the sharing of this data with any other state or private institutions, specifically health insurances, caused strong negative reactions.

Regarding data sharing between public institutions, several participants, mainly from focus group I (18-24 years), expressed rather ambivalent feelings: while on the one hand they perceived a number of advantages from the convenience of such a practice, at the same time they expressed a certain degree of anxiety regarding the likelihood that such a practice would effectively result in an increased level of control and interference into citizens' lives by the state. In contrast, members of focus group III (45+ years) perceived the sharing and exchange of data between public entities as a crucial tool for a properly functioning public administration system, especially with regards to the efficient functioning of the E-Government system.

Lastly, the sharing and selling of data between private entities was perceived as more problematic compared to data sharing between public entities. In particular, the respondents highly criticised the exchange and purchase of data between companies for their own economic advantage. Whilst most participants found this practice as generally acceptable as long as it was with the consumer's consent, participants perceived that such a practice still occurred without consent. Several participants expressed their helplessness and loss of control regarding the use of their data: "*I think you can't escape it*" (P6-I). As similarly stated by another participant, *"I think one can't do anything about it, when you give away these data and then the company decides to send them to another company"* (P5-I).

6. Conclusion

Throughout the different focus groups, the Austrian participants indicated a high awareness that individual citizens are indeed the subjects of surveillance in the main spaces considered during the discussion. The respondents also appeared to be well informed about the type of available surveillance technologies, not only on a national level but also internationally. In general, it appears that surveillance in commercial, boundary and public spaces has undergone a process of normalization, and technology-mediated surveillance is here considered as mostly acceptable for varying reasons, mainly for marketing purposes in relation to the commercial space and security-related purposes in all three spaces. On the other hand, in relation to the virtual space, it appears that the participants were unsure of which type of data is exactly being collected and by whom, an issue which also brought up concerns relating to citizens; rights in the virtual space.

With regards to the acceptance of technologically-mediated surveillance, it appears that different types of technologies meet varying levels of acceptance. While in general, CCTV and ANPR were considered as acceptable, the use of biometric data and location tracking – perceived as "*my most private things"* (P2-I) – was generally regarded as extremely invasive. The collection of such data was considered as a threat to privacy as well as increasing the risk of data misuse. With regards to locations of deployment, the Austrian participants considered surveillance as being generally acceptable in public places and unacceptable in what they perceived as private places.

Attitudes regarding the effectiveness of surveillance in combating crime were mixed. While some respondents argued that, in a way, surveillance technologies provide an effective antidote to '*anarchy'* (P3-I), others argued that surveillance should not be regarded as a cure to security-related issues, mostly because there are numerous ways to circumvent or neutralize surveillance measures. Seemingly, these participants suggested that rather than an intensification of surveillance, attention should be diverted to the social roots of crime. Additionally, the Austrian respondents expressed their resistance to being controlled by surveillance measures and declared their readiness to counteract such possible political development by a number of actions.

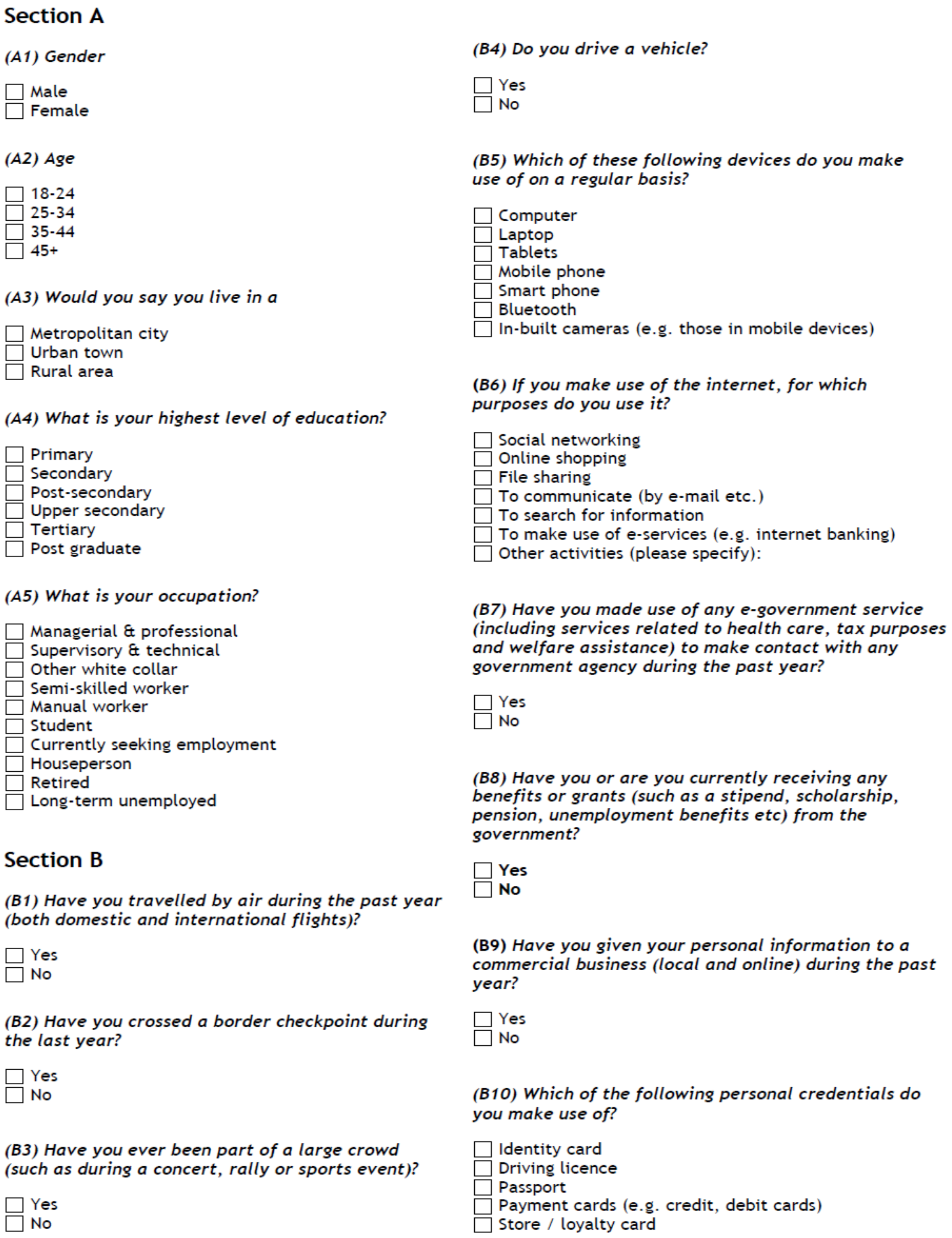
The majority of the participants expressed a general mistrust pertaining to surveillance measures. They perceived a risk of misuse, corruption and unlawful procedures mostly by private institutions. Interviewees expressed their helplessness and insecurity regarding the lack of transparency of surveillance procedures, privacy laws and personal rights, specifically in the virtual space. Thus, they strongly argued that more effort should be invested into the improvement of the current legal situation. Notwithstanding this criticism, several participants still expressed a significant level of trust in the state.

In conclusion, the Austrian participants sensed different violations of boundaries through the extensive use of surveillance measures. Ethical and social values appeared to be of high importance for the Austrians: "*My personal freedom and privacy is more valuable than security*" (P1-II). A deeply rooted resistance against monitoring and a general trend towards criminalization of citizens by extensive surveillance was expressed by several participants, who showed concern that such development could potentially lead towards dehumanization.

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*	***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**

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

knowledge of the technologies	***collect your personal information?***
2. Explore the participants' experience of being monitored in their many roles	***2. What type of information is being collected:*** ***a. What type of personal information do you think is being collected?***
3. Explore the participants' understanding of where their information is ending up	***3. Who is collecting the information:*** ***a. Who do you think is responsible for collecting and recording your personal information?*** ***b. Where do you think your personal information will end up?***
4. Explore the participants' views on why their actions and behaviours are observed, monitored and collected	***4. Why 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'...*

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

Aims

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

1. Participants' first reactions including:

Possibility / impossibility of scenario

Acceptability / unacceptability of

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?

scenario	***1d. Is such a scenario acceptable / unacceptable?***
2. Participants' beliefs and attitudes on how technology affects or might affect their privacy	***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?***
3. Participants' beliefs and attitudes in terms of the type of information such as: Medical & financial data; photos and location.	***3a. What type of personal information do you find acceptable to being collected, used and / or shared?*** ***3b. What type of personal information would you object to being collected, used and / or shared?***
4. Participants' beliefs and attitudes on the collection, usage and sharing of personal information with third parties.	***4a. What do you think about having your personal information collected, used and shared by the state?*** ***4b. What do you think about having your personal information collected, used and shared by private entities (such as commercial ones)?***
5. Participants' beliefs and attitudes on the benefits and drawbacks of being monitored	***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-off".* - *Here, the discussion should not focus on*	***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 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**

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

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)

2a. Which technologies do you consider acceptable? Why?

2b. Which technologies do you consider invasive 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?

3. Locations of deployment such as:
Airports
Malls
Streets

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

3b. Which locations do you consider unacceptable in relation to being monitored?

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

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

4b. Are there any safeguards or conditions that you would find reassuring?

5. Length of storage of surveillance data

5a. What do you think about the length of storage of surveillance data? Does it make a difference?

To help you probe, provide the following examples to the participants:

- ***Recordings of CCTV***
- ***The location and movement of cars***
- ***The storage of DNA, fingerprints and iris scans***
- ***The location of citizens who pose a risk to others***
- ***The location and movements of elderly people and children***

5b. If length of storage makes a difference, what would you consider as an acceptable timeframe?

Running Total: 1 hour 35min

Brief summary of discussion [5mins] ▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***Item 6 – Summing up session*** ***At the end of the focus group, it is helpful to provide a summary of the emerging points. Here you should aim at giving a brief summing up of the themes and issues raised during the discussion. After, you can ask for the following from the participants:*** - ***"How well does that capture what was said here today?"*** - ***"Is there anything we have missed?"*** - ***"Did we cover everything?"*** - ***This brief session will give participants an additional opportunity to express their views and can also be used to elaborate on topics raised but not pursued at the time.*** ***Running Total: 1 hour 40 min***
Conclusion of focus group **[5mins]** ▪ ***Thank the participants*** ▪ ***Hand out the reimbursement*** ▪ ***Give information on SMART***	***Item 7 –Closure*** **With this last exercise our discussion has come to an end. May we take this opportunity to once again thank you for joining us and for sharing your opinions, experiences and thoughts.** ***At this point, hand out the reimbursements to the participants and inform the participants about the next steps.*** ***Give out more information about the SMART to the participants requesting such information.*** ***Total: 1 hour and 45 min***

APPENDIX C – DISCUSSION GUIDELINES (AUSTRIAN)

Einführung	Einweisung
Begrüßung der Teilnehmer - *Teilnehmer begrüßen* - *Namenschilder erteilen* - *Einwilligungserklärungen unterschreiben lassen*	*Begrüßen Sie die Teilnehmer sobald Sie eintreten. Weisen Sie ihnen einen Platz zu und händigen Sie ihnen ihr* ***Namensschild*** *aus.* *Verteilen Sie die Einwilligungserklärungen an die Teilnehmer und bitten Sie sie diese zu lesen und zu unterschreiben,* ***bevor*** *die focus group startet. Dies ist wichtig um sicherzustellen, dass die Teilnehmer verstanden haben, wozu sie sich bereit erklärt haben.*
Einführung [ca. 10 min] - *Danke* - *Vorstellung des Moderationsteams* - *Zweck* - *Vertraulichkeit* - *Dauer* - *Grundregeln für die Gruppe* - *Kurze Vorstellung der Teilnehmer*	**Ich heiße Sie herzlich Willkommen zu dieser Gruppendiskussion und danke Ihnen, dass Sie sich bereit erklärt haben, bei dieser Befragung mitzuwirken.** **FRAGEBÖGEN** **EINWILLIGUNGSERKLÄRUNGEN** **Mein Name ist Agnes Rajkowska und ich werde die Gruppendiskussion moderieren. Ich werde hierbei durch meinen Co-Moderator Walter Hötzendorfer unterstützt, der sich ggf. Notizen machen und unsere Diskussion aufzeichnen wird.** *(Stellen Sie ggf. weitere, ebenfalls anwesende Kollegen vor.)* **Unsere Sitzung wird etwa eineinhalb bis zwei Stunden in Anspruch nehmen. Außerdem möchte ich euch bitten, klar und deutlich zu sprechen; eure Meinungen und Gedanken sind sehr wichtig für diese Untersuchung und wir würden ungern eine Bemerkung verpassen.** **Wie bereits anlässlich unserer ersten Kontaktaufnahme bezüglich eurer Teilnahme an dieser Diskussion erwähnt, beschäftigt sich diese Gruppendiskussion mit dem Thema „Technologie und Privatsphäre“ und findet als Teil des Projektes SMART, das von der Europäischen Kommission co-finanziert wird, statt. Diejenigen, die gerne mehr über das SMART-PROJEKT erfahren möchten, mögen sich bitte im Anschluss zu dieser Diskussion an uns wenden: wir sind gerne bereit, Ihnen weitere Informationen zukommen lassen.** *In dieser Phase ist es wichtig, keine weiteren Details über den Inhalt dieser focus group zu enthüllen, um eine Beeinflussung oder einseitige Betrachtungsweise zu vermeiden.*

Wie wir euch bereits mitgeteilt haben, wird alles, was bei dieser Befragung aufgezeichnet wird, vertraulich behandelt. Eure Identität wird anonym bleiben.

Die Informationen, die in den Abschlussbericht kommen, werden euch in keiner Weise als Teilnehmer identifizierbar machen. Um dies zu gewährleisten, haben wir jedem von euch eine Nummer zugewiesen und es wird diese Nummer sein, die im Abschlussbericht verwendet wird.

Ich würde auch gerne gewährleisten, dass jeder in der Gruppe sich wohl dabei fühlt, seine Meinungen zu äußern. Um dies zu ermöglichen, würde ich alle Anwesenden bitten, die folgenden Grundregeln zu beherzigen:

- **Da wir ein großes Interesse an den Auffassungen eines jeden von euch haben, würden wir auch gerne jeden von euch antworten hören. Gleichwohl seid ihr nicht verpflichtet zu antworten.**

- **Ich kann euch sagen, dass es keine richtigen oder falschen Antworten geben wird. Jeder von euch soll sich außerdem wohl dabei fühlen offen zu sprechen. Dafür ist es wichtig, dass wir die Ansichten eines jeden respektieren**

- **Damit die Diskussion nicht unterbrochen wird, stellt bitte sicher, dass eure Handys auf lautlos gestellt sind.**

- **Da uns jede einzelne Ansicht interessiert, ist es außerdem wichtig, dass auch die Kommentare einzeln und für sich abgegeben werden. Ich würde mich daher gerne mit euch darauf verständigen, dass wir nicht gleichzeitig sprechen, da es ansonsten schwierig für uns werden würde, alles was im Zuge dieser Diskussion geäußert wird, auch einzufangen.**

Wenn ansonsten einer von euch gerne irgendeine weitere Grundregel vorschlagen möchte, dann fühlt euch frei, eure Vorschläge jetzt der Gruppe zu unterbreiten.

Hat irgendjemand von euch noch irgendwelche Fragen, bevor wir starten?

In Ordnung, dann lasst uns damit beginnen, dass wir uns einander kurz vorstellen. Ich fange dann mal mit meiner Person an. Ich heiße Agnes Rajkowska und arbeite beim Projekt SMART mit. *(Nun zu meinem Co-Moderator..)*

Gesamtlaufzeit: 10 min

Zielen	Diskussionsthemen und Aufgaben

Wort-Assoziationsübung **[Ca. 5mins]** - *Wort-Assoziationsspiel dient als Aufwärmer* - *Vorrangige Assoziationen mit den Schlüsselthemen aufbauen* - *Diskussion starten*	***Item 1*** **Beginnen wollen wir mit einer Assoziationsübung: Ich werde ein Wort vorlesen und ich möchte euch bitten, die ersten paar Dinge zu sagen, die euch in den Sinn kommen, wenn ihr das Wort hört.** **Versucht nach Möglichkeit an einzelne Worte oder kurze Phrasen anstelle von längeren Beschreibungen zu denken.** **Lasst uns zunächst ein Beispiel ausprobieren:** **Was ist das erste, das euch in den Sinn kommt, wenn ich das Wort "Essen" sage?** **Gut. Dann wollen wir beginnen.** *Lesen Sie (einzeln) vor:* *Technologie, Privatsphäre, Nationale Sicherheit, Personenbezogene Daten, persönliche Sicherheit* *Gesamtlaufzeit: 15min*
Diskussion zu Alltagserfahrung mit Überwachung **[20min]** - *Erkunden, welche Erfahrungen die Teilnehmer mit Überwachung haben und wie sie diese wahrnehmen* - *Erkunden, inwiefern Teilnehmer sich der verschiedenen Überwachungstechnologien gewahr sind und was sie darüber wissen*	***Item 2*** **Lasst uns über etwas anderes sprechen. Ich möchte nun mit euch über Szenarien nachdenken, von denen ihr glaubt, dass ihr in irgendeiner Weise überwacht bzw. dass hierbei Informationen über euch gesammelt werden.** **Lasst uns die folgenden alltäglichen Szenarien als Beispiele dafür heranziehen.** **Szenario 1: Supermarkt - Als erstes Beispiel möche ich, dass ihr an einen Einkauf bei eurem örtlichen Supermarkt denkt. Könnt ihr uns eure Gedanken hierzu mitteilen? Glaubt ihr, dass Sie dabei überwacht werden bzw. Informationen von euch gesammelt werden? Falls „ja" wie und durch wen werden möglicherweise Information gesammelt? Welche Information werden gesammelt und warum werden diese möglicherweise gesammelt?** **Szenario 2: Reisen - Lasst uns bei gleichbleibender Fragestellung mit einer anderen Situation fortfahren, diesmal reisebezogen. Wie ist das, wenn ihr mit einem Flugzeug reist? Werdet ihr hierbei überwacht bzw. werden hierbei Informationen über euch gesammelt? Durch wen und wie? Warum werden diese Informationen gesammelt?** **Szenario 3: Öffentlicher Raum (e.g. Museum, Stadion) - Stellt euch nun vor, dass ihr eine öffentliche Einrichtung besucht, etwa ein Museum, oder dass ihr zu einer Veranstaltung wie einem Fußballspiel oder einem Konzert geht. Werdet ihr hierbei überwacht? Was wird möglicherweise überwacht? Wer überwacht euch und zu welchem**

Zweck?

Szenario 4: Mobile Endgeräte wie zum Beispiel Mobiltelefone - Lasst uns noch ein letztes Beispiel besprechen. Denkt über die Gelegenheiten nach, anlässlich derer ihr euer Handy benutzt. Was glaubt ihr wird in diesem Fall aufgezeichnet und wozu werden diese Informationen aufgezeichnet?

Ziele:

1. Erkunden, inwiefern Teilnehmer sich der verschiedenen Überwachungstechnologien gewahr sind und was sie darüber wissen
2. Erkunden, welche Erfahrungen die Teilnehmer mit Überwachung in ihren verschiedenen Rollen haben,
3. Erkunden, inwiefern die Teilnehmer verstehen, wohin ihre Daten gelangen?

4. Kennenlernen der Ansichten der Teilnehmer, warum ihre Handlungen und ihr Verhalten beobachtet, überwacht und gesammelt werden.

Hinsichtlich jeden Themas, und soweit relevant, fragen Sie nach, um die folgenden Details herauszuarbeiten:

1. ***Wie wird die Information gesammelt:***
   a. ***Welche Arten von Technologien werden Ihrer Meinung nach verwendet, um Ihrer persönlichen Informationen zu sammeln?***

2. ***Welche Art Informationen wird gesammelt**:*
   a. ***Welche Art persönlicher Informationen wird Ihrer Meinung nach gesammelt?***

3. ***Wer erhebt diese Informationen:***
   a. ***Wer ist Ihres Erachtens verantwortlich für die Erhebung und Aufzeichnung Ihrer personenbezogenen Informationen?***

   b. ***Was denken Sie, wohin Ihre personenbezogenen Informationen letztlich gelangen werden?***

4. ***Warum werden diese Informationen aufgezeichnet, gesammelt und gespeichert:***

   a. ***Warum denken Sie werden Ihre persönlichen Informationen gesammelt und aufgezeichnet?***

   b. ***Auf welche Arten werden Ihrer Meinung nach Ihre persönlichen Informationen genutzt werden?***

Gesamtlaufzeit: 35min

Präsentation der Karten, welche verschiedene Technologien und Anwendungen zeigen

Item 3

Mein Co-Moderator Walter wird euch nun die verschiedenen neuartigen Überwachungstechnologien erläutern.

Zeigen Sie die folgenden drei Karten (von denen jede eine Gruppe unterschiedlicher Technologien und Anwendungen abbildet) der

[10mins] *Den Teilnehmern eine Auswahl von relevanten SMART Technologien und Anwendungen vorstellen, um sie in die Lage zu versetzen, diese besser zu verstehen und so die Diskussion zu vereinfachen.*	*Gruppe. Die Karten werden die folgenden Abbildungen enthalten:* ***Karte 1 – Technologien zur Erkennung und Ortung von Personen und Ereignissen**: Automatisches Bewegen von Überwachungskameras; Automatische Nummernschilderkennung oder Automatische Fahrzeugnummernerkennung; sowie Ortung von Geräten wie Handy-Ortung oder RFID.* ***Karte 2 – Biometrische Systeme**: Biometrische Technologien einschließlich Fingerabdrucks- und Iris-Scannern; sowie automatische Gesichtserkennung* ***Karte 3 – Technologien zu Erkennung von Objekten und Produkten: Sog. “**Knife Arches” (Portalförmige Metalldetektoren z.B. an Flughäfen) und Röntgengeräte.* *Gesamtlaufzeit: 40min*

Präsentation eines MIMSI Szenarios gegenüber den Teilnehmern

[30mins]

- *Erkunden, inwieweit die Teilnehmer die Implikationen von MIMSI erfassen*
- *Gefühle, Auffassungen und Haltung der Teilnehmer gegenüber der Übermittlung personenbezogener Daten erkunden*

Item 4

Nun werden wir euch ein hypothetisches Szenario vorstellen. Dabei handelt es sich um ein Telefonat eines Herrn Braun mit einer Kundenbetreuerin des Arbeitsmarktservices, die wir Frau Schmidt nennen wollen. Ich werde die Rolle der Kundenbetreuerin Schmidt und Walter wird die Rolle des Kunden Braun übernehmen.

Stellen Sie der Gruppe das folgende, hypothetische Szenario vor. Es kann auch eine Aufzeichnung dieser telephonischen Unterhaltung vorbereitet und der Gruppe präsentiert werden.

Telephonat mit dem Kundenbetreuer bei der Zentralstelle der Bundesagentur für Arbeit

***Kundenbetreuer**: Guten Morgen, Schmidt hier. Wie geht es Ihnen, Herr Braun? Wir hatten eigentlich schon mit Ihrem Anruf gerechnet, nachdem Ihr Arbeitsvertrag bereits vor über einem Monat ausgelaufen war...*

***Herr Braun**: Äh, ja, das ist auch genau der Grund warum ich anrufe.*

***Kundenbetreuer**: Nun, es überrascht mich nicht, dass sie erst jetzt anrufen – wie war denn eigentlich Ihr Urlaub auf Zypern? Ihrer Frau und Ihren Kinder hat das Clubhotel bestimmt gefallen, oder?*

***Herr Braun**: Ja, war ein toller Urlaub... und woher wissen Sie all das?*

***Kundenbetreuer**: Nun, hab ich natürlich hier im System, Herr Braun. Wie dem auch sei, Sie sollten sich besser schnell daran machen, einen neuen Job zu finden… denken Sie an die Kosten Ihres Familienurlaubs und die Ratenzahlung für Ihren Wagen… nicht zu vergessen die VISA Abrechnung am 22. …*

***Herr Braun**: Wie, das haben Sie auch alles im System?*

***Kundenbetreuer**: Ja, selbstverständlich. Übrigens, das Buch, das Sie da online gekauft haben: eine gute Wahl! Hab es selbst gelesen und da waren ein paar echt gute Tipps dabei.*

***Herr Braun**: Hmmm...ok..noch mal zu diesem neuen Arbeitsvermittlungsdienst: brauchen Sie ein aktuelles Bild von mir?*

***Kundenbetreuer**: Nein, nein, darum haben wir uns selbstverständlich schon gekümmert! Wir haben jedemenge aktuelle Bilder in unserem System. À propos: sie haben gut Farbe bekommen im Urlaub. Das Wetter muss toll gewesen sein! Ah, bevor ich es vergessen, wegen des Bildes: bevorzugen Sie eines mit oder ohne Brille?*

***Herr Braun**: Oh...ja...also ohne Brille ist prima... also, wegen meiner Registrierung, könnten wir einen Termin für nächste Woche vereinbaren?*

***Kundenbetreuer**: Lassen Sie mich das kurz im System nachschauen…*

wie ist es Mittwoch mittag? Oh, moment, ich sehe gerade, Sie haben da schon einen Arzttermin. Den sollten Sie lieber wahrnehmen, denn Ihren Cholesterinspiegel überprüfen zu lassen ist sicher sinnvoll! Wie wäre es also mit Donnerstag, gleich als erster morgens um 9.00??

***Herr Braun**: Donnerstag morgen passt! Soll ich irgendwelche Dokumente mitbringen?*

***Kundenbetreuer**: Nein danke, Herr Braun, wir haben bereits alle Unterlagen, die wir brauchen, im System.*

***Herr Braun**: Das glaub ich gern…*

***Kundenbetreuer**: Danke für Ihren Anruf, Herr Braun, wir sehen uns dann nächste Woche. Ach, und genießen Sie ihren Cappuccino im Café Olé …*

***Herr Braun**: Das tue ich ... Auf Wiederhören!*

Zu diesem Szenario möchte ich euch nun einige Fragen stellen.

Nachdem Sie das vorstehende Szenario der Gruppe vorgestellt haben, forschen Sie weiter nach, um mehr über die folgenden Punkte zu erfahren:

Ziele
1. Direkte Reaktion der Teilnehmer, einschließlich:

Möglichkeit / Unmöglichkeit der Existenz eines solchen Szenarios

Akzeptabilität / Inakzeptablität eines solchen Szenarios

1a. Wie würdet ihr euch fühlen, wenn euch das passiert wäre? *(Forschen Sie auch nach, um den Grad an wahrgenommener Kontrolle / Hilflosigkeit der Teilnehmer in einem solchen hypothetischen Szenario zu eruieren.)*

1b. Wie würdet ihr reagieren, wenn euch das passiert wäre? Was würdet ihr tun?

1c. Hält ihr ein solches Szenario für <u>möglich oder eher unmöglich</u>?

1d. Wäre ein solches Szenario für euch <u>akzeptabel</u>?

2. Auffassungen und Einstellungen der Teilnehmer zu der Frage, inwiefern Technologie ihre Privatsphäre beeinflusst

2a. Inwiefern beeinträchtigen eurer Meinung nach herkömmliche Überwachungstechnologien eure Privatsphäre?

2b. Inwiefern beeinträchtigen eurer Meinung nach sog. "<u>smarte Technologien</u>", z.B. solche, die Daten <u>automatisch</u> oder halb-automatisch verarbeiten, eure Privatsphäre?

3. Auffassungen und Einstellungen der

3a. Hinsichtlich welcher Arten personenbezogener Informationen findet ihr deren Erhebung, Nutzung und oder deren Weitergabe <u>akzeptabel</u>?

Teilnehmer zu den Informationstypen wie etwa: Gesundheitsdaten, Finanzdaten, Photos und Ort.	***3b. Hinsichtlich welcher Arten personenbezogener Informationen würdet ihr Vorbehalte gegen deren Erhebung, Nutzung und oder deren Weitergabe haben?***
4. Auffassungen und Einstellungen der Teilnehmer zur Erhebung, Nutzung und Übermittlung von Personenbezogenen Daten an Dritte.	***4a. Was denkt ihr über die Erhebung, Nutzung und Weitergabe eurer personenbezogenen Informationen zwischen einzelnen verschiedenen Behörden (wie z.B. vom AMS an das Finanzamt)? Was denkt ihr über die Erhebung, Nutzung und Weitergabe eurer personenbezogenen Informationen zwischen verschiedenen Staaten?*** ***4b. Was denkt ihr über die Erhebung, Nutzung und Weitergabe eurer personenbezogenen Informationen durch Private Stellen (wie etwa Unternehmen)?***
5. Auffassungen und Einstellungen der Teilnehmer zu den Vor- und Nachteilen des Überwachtwerdens.	***5a. Glaubt ihr, dass es Vorteile haben könnte, eure Handlungen und euer Verhalten zu überwachen?*** ***5b. Glaubt ihr, dass es Nachteile haben könnte, eure Handlungen und euer Verhalten zu überwachen??*** *Gesamtlaufzeit: 1 Stunde 15min*

Reaktion auf Szenarien **[Ca. 20mins]** - *Stimulation einer Debatte, um die Wahrnehmung der Teilnehmer hinsichtlich des Verhältnisses von "Sicherheit vs. Privatsphäre" zu erkunden.* - *Die Diskussion sollte sich hier nicht darauf konzentrieren, inwiefern diese Technologien die Sicherheit tatsächlich erhöhen – das sollte als gegeben hingenommen werden. Die Diskussion sollte primär im Zentrum die Frage behandeln, ob diese Technologien die Privatsphäre beeinträchtigen und sich daher um das Verhältnis von Sicherheit zu Privatsphäre drehen.*	***Item 5*** **In der nächsten Übung werden wir ein hypothetisches Szenario diskutieren. Stellt euch folgendes Szenario vor:** *Aufgrund der erheblichen Zunahme von Gewaltverbrechen in der Hauptstadt, einschließlich einer Flut von Entführungen und Morden, die zufällig und ohne Verbindung zu sein scheinen, hat das Land beschlossen Videoüberwachung in allen öffentlichen Räumen, sowohl solcher, die der öffentlichen Hand gehören (U-Bahnen, Parks, öffentliche Toiletten), als auch solcher, die in Privateigentum stehen (etwa Geschäfte, Einkaufszentren, Taxis), einzurichten, welche eine automatische Gesichtserkennung ermöglichen wird. Daneben werden alle Fahrzeuge, die die Hauptkontrollpunkte passieren, anhand ihrer Nummernschilder registriert. Weiterhin gibt es Pläne, in allen öffentlichen Räumen Sensoren zu installieren, die laute Geräusche, wie etwa Schreie, erkennen können. Alle Bürger werden verpflichtet, Proben Ihrer DNA und Fingerabdrücke abzugeben, sowie die Iris scannen zu lassen. Das Land hat zudem entschieden, dass alle Bürger, die als mögliche Gefahr für andere identifiziert werden, sog. Elektronische Fußfesseln erhalten sollten, um ihre Bewegungen zu überwachen und aufzuzeichnen. Zu eurer eigenen Sicherheit, erhalten ältere Leute und Kinder bis zum Alter von 12 Jahren ebenfalls solche elektronischen Ortungsgeräte. Der gesamte Datenbestand dieser verschiedenen Technologien wird in vernetzten Datenbanken gespeichert, die durch die Polizei verwaltet werden, welche automatisch benachrichtigt wird, sobald ein Grund zur Alarmierung oder ein Risiko für irgendeinen Bürger besteht.* *Im Zuge der Diskussion des obigen Szenarios/ der Variationen, forschen Sie im Detail nach um mehr über die folgenden Faktoren und wie sie das Verhältnis "Sicherheit vs. Privatsphäre" beeinflussen:* ***1a. Was trägt in dem vorgestellten Szenario dazu bei, dass ihr***

euch sicher fühlt?

1b. Was trägt in dem vorgestellten Szenario dazu bei, dass ihr euch verletzlich fühlt?

Wandeln wir nun oben genanntes Szenario etwas ab:

Variation 1: Obwohl ein erheblicher Gewaltanstiegt in der Mehrzahl der Nachbarstädte zu verzeichnen ist, erlebt die Stadt, in der ihr lebt, keinen Anstieg der Kriminalität. Das Land entscheidet dennoch, die Überwachungsmaßnahmen als Vorsichtsmaßnahmen einzuführen.

Variation 2: Das gesamte Land hat eine sehr geringe Kriminalitätsrate insgesamt , das Land entscheidet aber dennoch die Einführung der Überwachungsmaßnahmen als Vorsichtsmaßnahme, nachdem in Einer Nachbarstadt (zB St.Pölten) ein Zwischenfall stattgefunden hatte, bei dem eine Anzahl Menschen niedergeschossen und ernsthaft verletzt wurde durch einen Mann, der in einem Einkaufszentrum das Feuer eröffnet hatte.

Ziele:

1. Sicherheitsklima und Bedrohungslage

2. Nutzung bestimmter Technologien

1c. Wärt ihr bereit eure Privatsphäre herzugeben, wenn die Gefahrenlage anders wäre, wie in Variation 1 und 2 des Szenarios?

2. Ich will nochmal die intelligenten Überwachungstechnologien des zuvor skizzierten Szenarios in Erinnerung rufen. In chronologischer Reihenfolge waren dies:

- ***Überwachungskameras mit automatischer Gesichtserkennung,***
- ***Automatische Nummernschilderkennung,***
- ***Sensoren (mit der Fähigkeit, laute Geräusche zu erkennen),***
- ***Biometrische Verfahren (einschließlich fingerabdrucksbasierte Verfahren)***
- ***und elektronischer Ortung (unter Nutzung von***

	RFID) 2a. Welche dieser Technologien findet ihr akzeptabel? Warum? 2b. Welche dieser Technologien empfindet ihr als in die Privatsphäre eingreifend und als Gefahr für diese? Warum? 2c. Was hält ihr von diesen automatisierten (oder halb-automatisierten) Technologien, bei denen die Letztentscheidung durch das System und nicht durch einen Menschen getroffen wird?
3. Anwendungsorte wie etwa: Flughäfen Einkaufszentren Straßen	3a. An welchen Orten fändet ihr die Überwachung eurer Person akzeptabel? Warum? 3b. An welchen Orten fändet Sie die Überwachung eurer Person inakzeptabel?
4. Existenz von Gesetzen und anderer Datenschutz-Sicherheitsmaßnahmen (in Bezug auf Erhebung, Speicherung und Nutzung von Daten)	4a. Was hält ihr vom Datenschutzrecht? Fühlt ihr euch dadurch geschützt? 4b. Gibt es irgendwelche datenschutzrechtlichen Sicherheitsmaßnahmen oder Bedingungen, die ihr als beruhigend empfinden würdet?
5. Dauer der Speicherung von Überwachungsdaten	5a. Was denkt ihr bezüglich der Dauer der Speicherung von Überwachungsdaten? Macht die Dauer der Speicherung einen Unterschied? Nennen Sie den Teilnehmern die folgenden Beispiele um das Gewinnen weiterer Erkenntnisse zu unterstützen: - Aufnahmen von Überwachungskameras - Ort und Bewegung von Fahrzeugen - Speicherung von DNA, Fingerabdrücken und Iris Scans - Aufenthaltsort von Bürgern, die für andere ein Risiko darstellen - Aufenthaltsort und Bewegungen älterer Leute und von Kindern 5b. Soweit die Dauer der Speicherung einen Unterschied macht, welchen Zeitrahmen fändet ihr akzeptabel? Gesamtlaufzeit: 1 Stunde 35min

Ziele	Zusammenfassung der Session

Kurze Zusammenfassung der Diskussion [5mins] ▪ *Bestätigung der wesentlichen der angeführten Aspekte* ▪ *Weitere Gelegenheit das Gesagte zu vertiefen*	***Item 6*** ***Am Ende der “focus group” ist es hilfreich, die herausgearbeiteten Punkte zusammenzufassen. Hier sollten Sie darauf abzielen, eine kurze Zusammenfassung der während der Diskussion aufgekommenen Themen und Problematiken zu geben. Danach können Sie die Teilnehmer folgendes fragen:*** - **“Wie gut gibt das wieder, was heute hier gesagt wurde?”** - **“Gibt es etwas, das wir vergessen haben?”** - **“Haben wir alles abgedeckt?”** ***Diese kurze Session wird es Teilnehmer ein weiteres mal ermöglichen, Ihre Ansichten zum Ausdruck zu bringen und kann zudem dafür genutzt werden, Themen, die zur Sprache kamen, aber vorher nicht weiter verfolgt wurden, zu vertiefen.*** ***Gesamtlaufzeit: 1 Stunde 40 min***

Ziele	Verabschiedung
Beendigung der focus group **[5mins]** ▪ ***Den Teilnehmern danken*** ▪ ***Auslagenerstattung*** ▪ ***Weitere Informationen zu SMART***	***Item 7*** **Mit dieser letzten Aufgabe ist unsere Diskussion an ihr Ende gelangt. Lasst uns diese Gelegenheit nutzen, euch ein weiteres Mal dafür zu danken, dass ihr teilgenommen und eure Ansichten, Erfahrungen und Gedanken mit uns geteilt habt.** ***Erstatten Sie nun den Teilnehmern die Auslagen und informieren Sie die Teilnehmer über die nächsten Schritte.*** ***Händigen Sie den Teilnehmern auf Verlangen weitere Informationen zu SMART aus.*** ***Gesamtlaufzeit: 1 Stunde 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. Loyalty cards

1.1.1.2. CCTV

1.1.2. Perceived purposes

1.1.2.1. Consumer behaviour research and marketing

1.1.2.2. Shelf, product and personnel organization

1.2. Boundary (border) space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. CCTV

1.2.1.2. Object and product detection devices

1.2.1.2.1. Luggage controls

1.2.1.2.2. Full body scanners

1.2.1.2.3. Knife and drug detectors

1.2.1.3. Monitoring of personal data

1.2.1.3.1. Passport control

1.2.1.3.2. Criminals record check

1.2.1.4. Biometric technologies

1.2.1.4.1. Fingerprinting

1.2.1.4.2. Facial recognition

1.2.2. Perceived purposes

1.2.2.1. National security

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV

1.3.1.2. Object detection devices

1.3.1.3. Monitoring of personal data

1.3.1.3.1. Identity checks

1.3.1.3.2. Personalisation of tickets

1.3.2. Perceived purposes

1.3.2.1. Prevention, detection and prosecution of crime

1.3.2.2. Crowd monitoring

1.3.2.3. Restrict access to registered troublemakers

1.3.2.4. Protection of property and artefacts

1.3.2.5. Marketing, statistics and resource management

1.4. Mobile devices and virtual spaces

1.4.1. Awareness of different surveillance methods/technologies

1.4.1.1. Recording of conversations (wiretapping)

1.4.1.2. Location tracking via GPS

1.4.1.3. Collection of data through smart phone applications

1.4.2. Perceived purposes

1.4.2.1. Prevention of crime

1.4.2.2. Tracing of criminals

1.4.2.3. Commercial purposes

1.4.2.4. Marketing and advertising

2. Perceptions and attitudes towards smart surveillance and dataveillance

2.1. Feelings

2.1.1. Extreme discomfort

2.1.1.1. Fear

2.1.1.2. Insecurity

2.1.1.3. Persecution

2.1.2. Physical discomfort

2.1.2.1. Feeling ‘naked’

2.1.3. Helplessness and resignation

2.1.3.1. Inescapability

2.1.3.2. Indignation

2.1.4. Anger

2.1.4.1. Violation of privacy

2.1.4.2. Opposition

2.2. Behavioural intentions

2.2.1. Active reactions

2.2.1.1. Immediate withdrawal

2.2.1.2. Counteracting

2.2.2. Self-protection strategies

2.2.2.1.1. Fool the system

2.2.2.1.2. Censoring

2.2.2.1.3. Disguise

2.2.3. Take legal action

2.3. Beliefs

2.3.1. Likelihood of smart surveillance and dataveillance

2.3.1.1. Technical aspect

2.3.1.1.1. Integration of data

2.3.1.2. Legal aspect

2.3.1.2.1. Imposed limits by current legislation

2.3.1.2.2. Trust into legislator

2.3.1.3. Ethical aspect

2.3.1.3.1. Notion of freedom

2.3.2. Perceived effectiveness of smart technologies

2.3.2.1. Convenience and risks of data sharing

2.3.2.2. Decision-making capabilities of automated systems

2.3.2.3. Human factor

2.3.2.4. Faster intervention possibility of smart technologies

2.3.2.5. Deterrent effect

2.3.3. The role of the state

3. Security-privacy trade-offs

3.1. Acceptance of technological surveillance

3.1.1. Feelings

3.1.1.1. Crossing of borders and violation of rights

3.1.1.2. Vulnerability: surveillance produces insecurity

3.1.2. General beliefs

3.1.2.1. Threat to freedom: association with communism

3.1.2.2. Observation of citizens: criminalisation of citizens

3.1.2.3. Safety and peace of mind: the “caring” function of surveillance

3.1.2.4. The satisfaction of a subjective feeling of security

3.1.2.5. Violation of privacy and freedom

3.1.3. Effectiveness of surveillance

3.1.3.1. Ineffectiveness for crime prevention

3.1.3.1.1. Alternatives to surveillance (e.g. Education)

3.2. Perceptions of different technologies

3.2.1. CCTV

3.2.1.1. Effect of normalisation

3.2.1.2. Inconspicuous nature of video-surveillance

3.2.1.3. Appropriate security measure

3.2.1.4. Conscience and intrusion: Change of behaviour

3.2.2. Biometric data and electronic tagging (RFID)

3.2.2.1. Strong perceptions of bodily/physical invasiveness

3.2.2.2. Sense of vulnerability: possibility of identity theft

3.3. Locations of deployment

3.3.1. Acceptable in public places: The ‘caring’ function of surveillance.

3.3.2. Unacceptable in private spaces and private spheres

4. Surveillance laws and regulations

4.1. Feelings and beliefs

- 4.1.1. A lack of information and transparency
- 4.1.2. Effectiveness of laws and regulations
- 4.1.3. Level of trust in the state
- 4.1.4. Level of trust in private actors
- 4.1.5. Length of data storage
- 4.1.6. Data sharing between different actors