European citizens' beliefs and attitudes towards smart surveillance and privacy

Noellie Brockdorff, Christine Garzia, Natalie Mundle
Department of Cognitive Science, University of Malta, Msida, Malta

May 2014

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

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

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

Table of Contents

1. Key Findings

This document presents the results of a qualitative study undertaken as part of the SMART project - "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727) - in the following 14 partner countries: Austria, Bulgaria, Czech Republic, France, Germany, Italy, Malta, Norway, Romania, Slovakia, Slovenia, Spain, the Netherlands and the United Kingdom. The analysis and results are based on 42 focus group discussions comprising of 353 participants, which were held in order to examine the beliefs and attitudes of citizens towards smart surveillance and privacy.

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

1.1 General findings

The following section delineates the general findings and common themes which emerged from the analysis of all 14 countries.

1. Participants were highly aware of being under surveillance in different contexts including commercial spaces, public places and boundary spaces such as airports. They were also knowledgeable about the wide range of surveillance technologies and methods employed in these contexts.
2. Participants were also rather knowledgeable about the extent of surveillance and the collection of citizens' data when making use of a mobile device. Similarly, most participants expressed their awareness of being systematically under surveillance in the virtual space. It appears that participants perceived a higher loss of control over personal data in this sphere.
3. Participants argued that individuals are, in part, responsible for divulging personal data, especially with regards to the virtual sphere. In particular, several participants criticised the naiveté of internet users in relation to online data sharing, especially on social networks.
4. Surveillance in public places and high risk areas was generally considered as acceptable, although a minority of participants did object to being monitored in public places. On the other hand, surveillance in private places was regarded as unacceptable. Participants also appeared to show a higher acceptance for surveillance when such monitoring was not covert. The lack of information available about implemented surveillance measures was criticised.

5. Participants perceived the surveillance of citizens and customers to take place either for security or for commercial purposes. Surveillance in public and boundary spaces for purposes of national security and citizen safety was generally considered as more acceptable than surveillance conducted by private companies for commercial objectives.
6. Participants typically perceived the extensive integration of data from dataveillance as a threat to citizens' privacy, and were thus generally against it. Nevertheless, acceptability appeared to be contingent on a number of factors, including type of data, purpose of use and whether consent was provided for data sharing. Concerns about risks of misuse and manipulation were also taken into consideration by the participants.
7. The collection and sharing of some types of data, some of it sensitive personal data, such as location data, financial information, as well as medical and health data, was deemed unacceptable by most participants. Nevertheless, it appears that in certain specific situations, especially in potentially life-saving circumstances, the use of certain types of confidential data was considered as justified.
8. The majority of participants considered the massive integration of personal data as technically possible, however, in most countries, it was perceived as currently unlikely due to legal restrictions or ethical constraints.
9. Acceptance of dataveillance appeared to be contingent on several criteria including purpose of data collection and use, whether consent was provided, type of data collected and shared, which entity – state or private – was conducting dataveillance and whether personal data was anonymised prior to being shared with third parties.
10. While participants typically perceived smart surveillance technologies as more intrusive compared to traditional surveillance measures, some argued that the use of smart surveillance could have less of a negative impact on privacy as well as decrease the risk of data misuse and manipulation.
11. Upon reflecting on the automated decision-making process of smart technologies, participants generally appeared sceptical of a wholly automated process devoid of human agency. Although participants pointed out that an automated process would be more objective, and thus more reliable than a surveillance process involving humans, they also argued that an automated process could possibly result in misinterpretations and in erroneous decisions being taken. In light of this, the majority of interviewees believed that the surveillance process should include a combination of technologically-mediated surveillance and human agency.
12. Different types of surveillance technologies typically met different levels of acceptance:
    i. The use of video-surveillance appeared to have undergone a process of normalization and participants generally tolerated its deployment in public places for security purposes.
    ii. The use of Automated Number Plate Recognition was generally tolerated, while the use of sound sensors was subject to mixed reactions.

iii. The use of biometric technologies and electronic tagging, hence surveillance involving the physical sphere, was perceived as extreme and deemed unacceptable.

13. Extensive surveillance was perceived as posing a threat not only to privacy but also to the freedom of citizens. Concerns were also expressed by the participants in relation to the possible abuse of power by the state, since the collection of surveillance data was regarded as creating a power imbalance between the state and its citizens. Other perceived concerns resulting from the use of extensive surveillance included the possibility that monitoring could facilitate processes of dehumanisation in society. The intensification of surveillance was also considered as labelling each citizen as a potential risk, and thus as possibly resulting in a general criminalisation of citizens.

14. The majority of participants rejected the concept that extensive surveillance would result in increased security. The surveillance of citizens was not seen as a viable solution for the reduction of crime and therefore most participants were not willing to sacrifice their privacy for increased surveillance in case of a rise in crime. Alternative options to surveillance, such as the use of education, were suggested by several participants.

15. Participants perceived a variety of threats deriving from surveillance, including the use of surveillance tools by the state as a means to control citizens and a higher risk of misappropriation of surveillance data. As a consequence, rather than enhancing feelings of personal safety, an increase in surveillance measures resulted in feelings of deep insecurity.

16. Participants strongly questioned the effectiveness of surveillance measures in relation to the deterrence and prevention of crime. On the other hand, surveillance appeared to be considered as effective for the investigation of crime.

17. The majority of participants displayed a lack of knowledge of privacy laws and regulations. The participants mainly attributed this lack of knowledge to the perceived complexity of the legal jargon used and a general lack of initiative by citizens in getting informed about the legislation.

18. While some participants regarded current privacy legislation as inadequate and also as outdated due to the fast advancement of technology, others appeared satisfied with the level of protection offered by privacy legislation.

19. Expectations regarding ideal length of data storage for surveillance data varied. While some participants appeared to prefer a relatively short storage time ranging from hours to weeks, others stated that surveillance data should be stored for months, years or even indefinitely in certain cases. Additionally, some participants appeared indifferent to length of data storage. Overall, participants suggested several criteria which in their opinion should determine storage period, including type of data and purpose of use. In relation to the latter, it appears that most participants were in favour of a relatively longer storage period in case surveillance data is utilised for purposes of crime investigation.

20. Whilst on the one hand acknowledging that the storage of surveillance data is useful in investigation and prosecution of crime, on the other hand it appeared to be a cause for concern amongst the

majority of participants since this was regarded as increasing risks of data misuse and misappropriation.

21. Data sharing between public actors for security or administrative purposes was considered as more acceptable than the sharing of data between private actors for commercial purposes.

1.2 Country Highlights

The following are findings that were particularly prevalent in individual countries and which differed from findings overall. These results are not described in this report but are discussed in full in the relevant individual country reports produced as part of this study.

1. **Austria**: Trust in the government and existing legislation, as well as into the country's ethical and social values was high. Nevertheless, participants perceived various risks deriving from the use of surveillance procedures and therefore argued that more effort should be invested into strengthening the current legal framework in order to protect citizens' rights.

2. **Bulgaria, Slovakia:** There appeared to be a low level of trust in the legal protective mechanisms provided by the state and participants appeared dissatisfied with the current legal measures in relation to privacy.

3. **Czech Republic, Germany, Slovenia, and The Netherlands:** Contrasting opinions with regards to the effectiveness of the legislation were evident; while some claimed that they feel protected by the existing legislation, others expressed their misgivings about the effectiveness of the legal mechanisms in place.

4. **France:** It appears that the majority of participants trusted the authorities with the collection and use of citizen data, with the main belief being that unless there is a valid justification, citizens are not the target of extensive surveillance. Most participants thus appeared unconcerned that the state could misuse surveillance data.

5. **Italy:** Participants appeared particularly sceptical vis-à-vis the use of extensive surveillance for dealing with security-related concerns. It was argued that such measures fail to address the core of the problem and that surveillance could be easily circumvented or neutralised. In view of this, some participants advocated the use of alternative measures; more specifically they argued that there should be an emphasis on prevention which is based on social, rather than technological means.

6. **Malta:** Most participants appeared to have a low level of trust in the Maltese judicial system. Specifically in relation to privacy legislation, it appears that they do not feel sufficiently protected by

the Data Protection Act. Two major problems highlighted by most participants were the lack of enforcement by the authorities and the existence of loopholes in the legislation.

7. **Norway:** Participants' main concerns in the context of personal data collection on a massive scale and in combination with long-term storage were twofold: While they did perceive increased data security issues, what appeared to concern them more was the gradual build-up of a complex data-based "digital collective memory" which may not be as merciful and forgiving as human memory. In view of this, participants highlighted the need for a strong and independent data protection authority.

8. **Romania**: Views on the use of surveillance amongst the participants were polarised; while a number of participants willingly accepted a decrease in privacy for increased personal safety and public security, others expressed a deep sense of vulnerability and unease at the use of extensive surveillance. Rather than placing their trust in surveillance, the latter participants stated that what reassures then is the country's moral fibre.

9. **Spain:** Although participants perceived the existing legal framework as providing sufficient protection for citizens, participants believed that legislation needed enforcement in order to be efficient.

10. **United Kingdom:** Interviewees showed particular scepticism at the law's effectiveness in the prevention of misuse of citizens' data. It was perceived that legal safeguards could be circumvented by powerful interests.

2. Introduction

The analysis and results in this document are based on 14 countries with 3 focus groups each 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.

This document synthesises the findings from all participating countries. Separate country-specific reports are available for the following 14 countries: Austria, 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[2]. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research project.

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.

[2] It should be pointed out that during this period, two major world events occurred: firstly, the Boston Marathon Bombings, which occurred on the 15th April, 2013, and secondly, the revelations made by Edward Snowden with regards to the mass surveillance programmes undertaken by the National Security Agency (NSA), which came to light in the international media in June, 2013. Although the majority of the focus groups were carried out before these events, some focus group sessions were conducted after. Albeit difficult to ascertain, it does not appear that these occurrences influenced the participants' views on government surveillance as these did not differ between focus groups carried out before and after these events.

3.2 Discussion guidelines

Discussion guidelines (see Appendix B for the discussion guidelines in English) 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 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.

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 C) at the end of each session.

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

All focus group sessions, which were audio-recorded in order to be transcribed, were conducted in the local language. In general, the duration of the sessions was around 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 re-categorising 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.

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. Further to the finalisation of all 14 country reports, this final report was drafted. The aim of this final report is to summarise the results of the study, to highlight the key findings as well as to indicate any country differences which emerged.

4. Results

4.1 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.

4.1.1 Commercial Space

The vast majority of participants generally displayed a high awareness of the presence of different surveillance devices in the commercial space, including video-surveillance systems, the use of loyalty cards, financial monitoring and theft detection devices. In all countries, the use of CCTV systems was mentioned as a predominant surveillance measure with its main perceived purpose being theft prevention. Overall, this appeared to be a justified security measure which was widely accepted by participants. Recordings were perceived to be watched by security companies or by the police predominantly in the case of an incident. Exposure to surveillance in commercial spaces was seen by many participants as a matter of personal choice since entering a commercial space was ultimately regarded as an individual's decision.

In relation to loyalty cards, the majority of participants perceived them as being primarily directed at monitoring overall patterns of consumption and customer behavior for marketing and advertising purposes. The majority of participants indicated a general acceptance towards the use of their data for market research purposes since as customers, they perceived a number of benefits deriving from such practices. Italian participants were particularly accepting of the collection and use of their data due to the belief that consumers voluntarily choose to register for a loyalty card. However, the collection of personal data for the creating of databases seemed to raise a certain discomfort amongst the participants of all countries and concerns were expressed in relation to the further use of their data and its dissemination. Lastly, financial monitoring, such as the surveillance of debit or credit card movements, was perceived as rather suspicious, since it was unclear to participants who would use this data and for what purposes.

4.1.2 Boundary Space

In the context of border control, the discussion mainly focused on an airport setting as a boundary space. Here, surveillance was considered as ubiquitous and inescapable, and the predominant sentiment was that in this space surveillance is justified, and hence acceptable, for security reasons. In this context, participants of all countries perceived national security and passenger safety as being the predominant purposes of surveillance. To a much lesser extent, some participants additionally mentioned commercial motivations and functions related to the collection of statistics and of personal customer data.

In line with the pervasiveness of surveillance in this space, a variety of surveillance methods was mentioned by the participants. The use of video-surveillance, mainly traditional CCTV systems, as well as biometric technologies, such as fingerprinting and retinal scanning were considered as being widespread in this context. The use of smart CCTV with automatic facial recognition (AFR) was also mentioned by some of the participants. While the use of biometrics in this sensitive context appeared to be tolerated by most of the participants in the majority of countries, it appears that in certain countries, including Bulgaria and Slovakia, biometric surveillance raised a certain level of discomfort amongst the participants.

Participants also mentioned a number of object and product detection devices, such as luggage controls, metal detectors, x-ray machines and full body scanners. The monitoring of personal data was also considered as occurring via several means including the purchase of flight tickets, financial monitoring, passport control, visa applications, checking of passenger data against criminal records, passenger lists or the airline booking system. In addition to technological surveillance, some participants also mentioned surveillance by airport personnel trained to look out for certain behaviour and also the use of sniffer dogs.

Overall it appears that participants were generally aware of being surveilled by a variety of entities including airport security services, commercial entities such as airline companies and travel agencies, different government authorities such as law enforcement agencies and customs officers, foreign governments and international agencies such as Interpol. In particular, the Spanish participants expected airports to collaborate and exchange data with different national agencies, including law enforcement agencies, in order to guarantee security.

As mentioned earlier, national security and traveller safety were seen as the primary purposes of surveillance in all countries. In particular the prevention of crimes by the prior identification of criminals or dangerous suspects was mentioned, especially those linked to terrorism. Participants also pointed out the possibility that surveillance at airports can be used as a means to control national borders, for instance in order to detect individuals, such as criminals, who are prohibited from entering or leaving the country. Lastly, some participants from several countries argued that the extent of surveillance at

airports is dependent, in part, on the country in question and most participants perceived surveillance measures in the European Union to be less intrusive than in countries such Israel and the United States.

4.1.3 Common Public Spaces

In common public spaces, such as in museums, train stations, or in stadiums and town squares where mass events like concerts and sport events are organised, participants in all countries generally mentioned a range of methods through which surveillance occurs. The use of CCTV was perceived as a primary means of surveillance in this context in all countries. In case of mass events, participants from some countries, including Malta and France, also mentioned the possibility of being inadvertently recorded by any television cameras filming the event. In addition to technological surveillance, reference was also made to the presence of security officers and law enforcement personnel. The use of turnstiles at the entrance of the venues as a means to monitor the flow of the visitors was also mentioned in Spain. The monitoring of personal data via the purchase of tickets and ID checks upon entrance to the event was also pointed out in most countries.

In general, the predominant functions of surveillance in public places were perceived as being public security, citizen safety and the protection of property. These purposes were regarded as justified and were accepted by the majority of participants. Surveillance data was believed to be collected by state authorities, primarily law enforcement agencies, as well as by private entities, mainly the event organisers and private security companies. Participants discussed a number of different purposes of surveillance in public places including organisational and security purposes, such as the prevention and detection of incidents in order for security personnel or law enforcement officers to be able to intervene in a timely manner. Additionally, the use of video-surveillance was regarded as a tool for crowd monitoring and for the regulation of visitor flows. Lastly, with particular reference to public institutions such as museums, some participants mentioned the use of surveillance for the protection of property and artefacts and to prevent theft and vandalism.

4.1.4 Mobile Devices and Virtual Spaces

Participants appeared to be aware of the extent of surveillance when making use of a mobile device and mentioned a range of methods through which technologically-mediated surveillance occurs, or can potentially occur, within this context. The most frequently mentioned methods were the monitoring of call and message lists, location tracking through GPS, and the recording of conversations. Moreover, participants in several countries, mainly in Austria, France, Germany, Malta, Romania, Slovenia and The Netherlands, discussed the collection of data through the use of Bluetooth and Wi-Fi networks as well as via smart phone applications.

Perceived purposes of monitoring in this context differed according to the type of data gathered. It can be noted that surveillance data was here perceived by the majority of participants as being used for two main purposes. Firstly, the recording of conversations and location tracking via GPS were regarded as being carried out for security-related purposes in rather atypical circumstances which would usually necessitate a warrant. In general, participants stated that such monitoring tools provided law enforcement agencies the means to prevent and fight crime, such as the identification of suspicious behaviour. In addition to the likelihood that customer data is passed on to law enforcement agencies, participants additionally mentioned other third parties with whom such data could potentially be shared, including advertisers, phone manufacturers and other government entities. Dutch participants in particular appeared concerned about the possibility that such data sharing could result in data theft and misappropriation. Consequently, surveillance data was considered as valuable for marketing and advertisement purposes, and the collection of data was thus perceived as a lucrative practice.

There was particular unease amongst Austrian, German, Italian and Maltese participants regarding the surveillance of smart phones and online services. Participants were especially concerned about the permanency of data traces and the possibility of misuse in this context. In addition, personal rights in the virtual space and the protection of privacy were perceived as unclear, which resulted in feelings of helplessness amongst some of these participants.

4.2 Perceptions & Attitudes towards Smart Surveillance and Integrated Dataveillance

One of the central tasks of this study was to research citizens' feelings and beliefs on smart surveillance and massively integrated dataveillance, the latter referring to "*the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*"[3]. In order to elicit the attitudes towards massively integrated dataveillance, participants were presented with an everyday scenario: a recorded telephone conversation between a job seeker and a civil servant of the employment agency, where complex surveillance[4] becomes evident.

4.2.1 Feelings

After having listened to this conversation, in all countries participants expressed strong negative reactions and revealed feelings which predominantly indicated disbelief and shock, an extreme sense of discomfort, fear, as well as a sense of helplessness and resignation. Some participants also experienced indignation, outrage and anger at what they perceived was a serious violation of privacy. On the other hand, a slight minority perceived the extensive collection and massive integration of data as convenient in relation to the facilitation of bureaucratic procedures.

4.2.2 Behavioural Intentions

In addition to asking about their feelings upon listening to this conversation, participants were also asked for their resulting behavioural intentions. Some participants suggested a rather passive reaction involving some kind of immediate withdrawal from the hypothetical situation, such as hanging up the phone. This passivity, which was particularly evident in Italy, Romania and Slovakia, appears to indicate a sense of helplessness and resignation. This contrasts sharply with the proactive reactions of some participants, most notably from Malta and Slovenia, who claimed they would have questioned the civil servant there and then about how their personal data was obtained.

Actions of a precautionary nature were additionally mentioned by participants from Austria, Bulgaria and Slovakia, which mainly targeted a change in behaviour. These included self-censoring and the adoption of a more careful approach when divulging personal information, most notably in relation to online behaviour, as well as a change in day-to-day behaviours such as paying in cash rather than using a credit card in order to avoid financial monitoring and reducing the use of mobile phones.

Several participants from the majority of countries stated that they would engage in different measures in order to counteract such a situation. Perceiving the massive integration of data as illegal, several

[3] Clarke, R. (1997)

[4] The statements of the civil 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

participants in most countries claimed they would either report the incident to the relevant local authorities, most notably the Data Protection Agency, or else resort to legal assistance by personally contacting a lawyer. At the same time, however, some participants, particularly from Spain, appeared intimidated by the idea of initiating legal action against the state and expressed doubt as to whether this would indeed be effective.

4.2.3 Beliefs

4.2.3.1 Likelihood of integrated dataveillance

Regarding the likelihood of whether or not smart surveillance and massively integrated dataveillance are possible (currently or in the future), participants generally distinguished between technical, ethical, and legal aspects.

Generally, the development of massively integrated dataveillance was perceived by participants from the majority of countries to be certainly possible from a technical aspect, albeit not to the extent as portrayed in the scenario, which was considered as somewhat excessive and exaggerated. Slovenian and Dutch participants argued that to a certain degree the massive integration of data from different sources is already a reality. Nevertheless, although technically possible, several participants questioned the likelihood of massively integrated dataveillance from a legal perspective, since they perceived such practices as illegal. Moreover, ethical considerations were brought up by the participants who perceived the massive integration of data as unacceptable primarily due to privacy reasons.

Participants believed that the rapid development of surveillance technologies could eventually lead to extensive dataveillance. In spite of this, however, Slovakian participants appeared sceptical that the massive integration of data would occur in the near future in their own country due to the perception that, in comparison to other countries, technical capacities were less developed in Slovakia.

In addition, participants expressed a strong belief that the likelihood of massively integrated dataveillance taking place would depend to a certain extent on individuals' self-responsibility in divulging their personal information. Several participants argued that the blame rests with the individuals themselves who voluntarily divulge their personal data in an irresponsible manner. The discussion here mainly revolved around self-responsibility in the context of virtual spaces and on-line social networks.

Nevertheless, although technically possible, several participants questioned the likelihood of massively integrated dataveillance from a legal perspective. In the Austrian, Norwegian and Spanish groups, many participants expressed their trust in the local legislative framework which they regarded as providing a suitable protective mechanism in relation to citizens' privacy. On the other hand, Slovakian and German

participants appeared rather mistrustful of the state's intentions and appeared to believe that the state monitors its citizens extensively. In other groups, including the French and Austrian ones, participants did not exclude the possibility that future legal developments could result in such practices becoming permissible.

Lastly, in most countries it was argued that the spread and intensification of surveillance is not merely a technical and legal issue. Several participants, most notably from Austria, Czech Republic, Italy and Malta, argued that the likelihood of massively integrated dataveillance is unlikely since it is unacceptable from an ethical standpoint, not only in relation to privacy but also in relation to citizens' freedom.

4.2.3.2 Acceptance of integrated dataveillance

After discussing the likelihood of massively integrated dataveillance, the participants also discussed its acceptability. As mentioned previously, the majority of participants in all countries regarded the scenario as unacceptable, primarily due to the perception that the integration and use of data from several sources involved a serious violation of privacy. In addition to privacy issues, extensive surveillance was believed to create a power imbalance between citizens and the state. This was perceived as a threat to citizens' freedom since the use of surveillance was regarded as an opportunity to manipulate and control the lives and activities of citizens. At the same time, however, some participants argued that surveillance is, to a certain extent, undergoing a process of normalisation and, in some countries, including France and Slovakia, participants expressed concern that a possible shift in societal values could result in such practices becoming acceptable.

Overall it appears that participants' acceptance of massively integrated dataveillance depended on a number of factors. In general, it seems that a major factor influencing acceptability was purpose of use of surveillance data. Participants in all countries stated their acceptability of dataveillance vis-à-vis general public security measures and especially for investigating crime. Amongst some British, French, Maltese, and Slovenian participants dataveillance was also perceived as acceptable in cases where it was considered as enhancing service efficiency and as facilitating user convenience especially in relation to bureaucratic procedures.

Two other aspects which had a bearing on the acceptance of dataveillance were type of data to be stored and shared and whether consent for data sharing was provided by the citizen. The personal data which participants generally objected to sharing included location data, financial information as well as medical, health and genetic data. Norwegian participants were especially concerned about the gradual build-up of a complex collection of personal data of individuals which could be used against citizens. Nevertheless, it appears that in specific situations, especially in potentially life-saving circumstances, the use of certain types of confidential data, such as medical data, was considered as justified. Secondly, in several countries, including Austria, Bulgaria, Germany, Malta, Romania, Slovakia and The Netherlands,

participants argued that unless consent is expressly given, the sharing of personal information would be deemed as unacceptable. It appears that participants were rather aware of covert practices of data sharing and this resulted in feelings of insecurity.

Lastly, participants discussed the collection, use and sharing of data by state entities and by private organizations. Attitudes on data sharing by the state were noticeably mixed; whereas some participants were of the opinion that the state was more trustworthy in this regard, others did not show much trust in the authorities. In fact one of the main concerns expressed by some participants, especially in Slovenia and in Spain, was the possibility that the state would collect and store citizen data in a central database which could then be made accessible to all public authorities. On the other hand, in relation to private entities a typical pattern could be noticed in all countries; participants generally expressed negative reactions since they regarded data sharing without consent as a rampant practice in the private sector. Overall participants expressed a lack of trust in private organizations since commercial interests were perceived as the major driver for such entities. Lastly, not only did participants perceive a stronger violation of privacy in relation to data sharing amongst private actors, but they also regarded such practices as resulting in increased risks.

4.2.3.3 Perceived effectiveness of smart technologies

Issues of effectiveness were also mentioned by the participants, who primarily discussed the automatic decision-making process of smart technologies. It appears that the issue of automation brought up mixed feelings and beliefs amongst all participants. Firstly, the participants differentiated between decisions taken by humans and those taken by automated technologies. In this regard, a number of participants stated that humans introduce an element of subjectivity and bias into the surveillance process, and therefore proceeded to argue that the use of fully-automated systems would result in a more objective decision-making process. However, this viewpoint was challenged by participants who argued that such systems are nevertheless programmed by humans and that human biases could be transferred to the machine through the programming process. On the other hand, some participants appeared to be sceptical and distrustful of technology on its own without human agency and expressed unease at the risk that smart technologies could erroneously assess or interpret a given situation.

Notwithstanding these divergent viewpoints, it appears that the majority of participants preferred a surveillance process which comprises of the technological as well as the human element, and where the final decision is executed by a human being.

4.3 Security-Privacy Trade-offs

4.3.1 Acceptance of Technological Surveillance

In order to gauge participants' perceptions vis-à-vis the security-privacy trade-off, as well as their attitudes towards a number of specific smart technologies, a hypothetical scenario was presented to participants. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging of convicted criminals and of vulnerable individuals such as children and the elderly. The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[5].

When discussing the scenario, the majority of participants displayed very intense reactions, perceiving the use of all the aforementioned surveillance measures in conjunction as frightening and excessive. In several countries, including Italy, Malta, Romania, Slovenia and The Netherlands, participants argued that with the introduction of intensive surveillance, a democratic state could easily develop into a 'police state'. In fact, rather than enhancing feelings of personal safety, the security measures portrayed in the scenario resulted in feelings of discomfort and insecurity amongst most of the participants.

A number of reasons can be attributed to such heightened feelings of vulnerability and unease. Firstly, a number of participants expressed concern at the way that surveillance measures affected their privacy, perceiving surveillance technologies as providing a means through which one is constantly monitored. Secondly, several participants appeared to believe that once such measures are introduced, the intensification of surveillance would undoubtedly continue to escalate and possibly shift from monitoring criminals to observing all citizens. Such a perceived power imbalance between the citizen and the state was not only seen as severely impinging on privacy but also brought up concerns related to the freedom of citizens. Such a restriction on freedom was regarded as a potentially dangerous development not only for individual citizens but for all of society. In this regard, some participants argued that surveillance tools could be employed for the unjustified monitoring and control of citizens, with security being used as a pretext to disguise any hidden agendas by the state. Moreover, in some countries, most notably in Italy and Malta, some participants argued that in case of a change in the national political scene, methods of intensive surveillance could potentially be used against the interests of citizens.

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

Another major reason why the extensive use of surveillance as described in the hypothetical scenario was considered as generally unacceptable was the anxiety caused by the perceived possibility of misappropriation and misuse of surveillance data, as well as the risk of corruption, which would lead to several negative consequences for citizens. Specific fears mentioned by participants included the manipulation of digital evidence as well as possibly becoming victims of discrimination and identity theft.

The predominant belief amongst participants was that security could never be fully guaranteed, with several participants doubting and challenging the notion that technological surveillance was the best solution to reduce or eliminate crime. In this regard, several participants pointed out that countless ways and means exist to circumvent and neutralise surveillance. Whilst most participants acknowledged that the use of technology could be useful for the purposes of investigation of crime, opinions on whether surveillance would be effective in terms of prevention and deterrence of crimes were decidedly mixed. While some participants stated that to a certain extent some criminal acts might be prevented by the use of surveillance measures, it appears that the majority argued that surveillance will not act as a deterrent.

In light of such beliefs, several participants, from all countries but especially from Germany and Italy, were sceptical about the use of extensive surveillance to increase security, because these measures were perceived as failing to address the core of the problem. In fact, several participants from Italy, Malta, Romania, Slovenia and Spain, argued that rather than the use of intensive surveillance and control, effort should be invested in education. Consequently, even when faced with versions of the scenario depicting a marked increase in crime, participants were still of the opinion that extensive surveillance measures could not be justified, with only a minority expressing their confidence in surveillance measures and perceiving them as having the potential to increase personal safety and public security by providing law enforcement personnel with tools to fight criminals.

4.3.2 Perception of Different Technologies

Different types of surveillance technologies seemed to meet different levels of acceptance in all countries. While the use of video surveillance, sound sensors and Automatic Number Plate Recognition (ANPR) was on the whole considered as acceptable by the majority of participants, the use of biometric data and especially electronic tagging was, with few exceptions, considered as unacceptable. It appears that participants from several countries found difficulty in understanding the operational nature of smart technologies.

The use of traditional CCTV systems appears to have undergone a process of normalisation; this technology was considered not only as acceptable but also as necessary in certain locations, with very few participants objecting to the use of video surveillance in public places. In general, most participants highlighted the widespread use, as well as the inconspicuous nature of video-surveillance, as a potential

reason for acceptance. Nevertheless, in relation to smart CCTV, it appears that the function of automatic face recognition (AFR) was perceived by many participants as breaching citizens' privacy. Similar to the use of traditional CCTV, the use of ANPR was overall considered as acceptable. Additionally, while the use of sound sensors was perceived as generally acceptable, at the same time it appears that many participants had mixed feelings with regards to the effectiveness of this surveillance measure. While some perceived them as an efficient security measure in preventing crime and enabling quick police intervention, others argued that the use of this technology could result in wrong conclusions being drawn and mentioned instances of people raising their voices or children screaming.

In contrast to the above attitudes, the use of biometric data and electronic tagging – hence surveillance involving the physical sphere – was in general considered as extremely intrusive. Overall, participants seemed to feel a heightened sense of vulnerability in relation to biometric surveillance since the collection of this type of data was perceived as presenting a higher threat to privacy. From the different types of biometrical data portrayed in the scenario it appears that the most sensitive type was DNA data since such data was seen as providing information on health and genetics. Various concerns were raised by the participants including the possibility of identity theft.

The use of electronic tagging brought about the strongest reactions amongst the participants in all countries. Deemed as particularly excessive and as extremely intrusive, most participants objected to the use of this surveillance tool not solely due to privacy reasons but also due to the belief that tagging could lead to being controlled in daily life. Consequently, many pointed out at the loss of freedom that such use would entail, with the possibility that this could lead to a sense of dehumanisation. With regards to the tagging of vulnerable groups in society including the elderly and children, opinions were mixed. While the participants strongly opposed the mandatory tagging of elderly people, it appears that if electronic tagging was done on a voluntary basis it was then considered as acceptable, especially since the use of such a tool could be life-saving in emergency situations. The tagging of children was subject to different opinions; while some did not object to the use of tagging since it would provide parents with a certain 'peace of mind', others considered the tagging of children as being totally unacceptable since they argued that monitoring children in this way would be detrimental to their psychological development. Lastly, in relation to the use of electronic tagging exclusively for criminals, the majority of participants, with some exceptions, appeared to be accepting of such use. In particular, the French participants were in favour of criminals being electronically tagged for a certain amount of time after they left the prison.

, Overall participants accepted the deployment of surveillance devices in public places, especially in places experiencing large flows or masses of people, and in places considered as high risk areas, such as airports and train or underground stations. It appears that in general, surveillance in public places was considered as part of the 'caring' function of surveillance. In contrast, surveillance in private spaces was

considered as unacceptable by most participants because it was perceived as presenting a violation of privacy and also as impinging on citizens' freedom.

4.4 Surveillance Laws & Regulations

4.4.1 A lack of information and transparency

A lack of knowledge vis-à-vis the content of legislation was evident amongst the majority of participants in all countries. Some participants ascribed this lack of knowledge to the difficulties faced by laypeople in understanding legal jargon. In light of this, some participants suggested that legal information should be provided to citizens in a more straightforward and transparent manner. Moreover, while some participants also pointed out the lack of initiatives aimed at raising awareness and educating citizens about privacy, others argued that the lack of interest by citizens in getting informed about their privacy rights was a part of the problem.

4.4.2 Trust in the state and effectiveness of legislation

Opinions were somewhat divided on the effectiveness of, and protection offered by privacy legislation. In this respect, it should be borne in mind that as mentioned above, the participants' limited knowledge and awareness of privacy laws might have made it difficult for them to determine whether the existing laws and regulations do indeed offer the required protection.

Some participants, in particular those from Austria and Spain, stated that they do feel protected by current legislation and appeared to trust the state's Data Protection Agency. In fact, the participants pointed out citizens' responsibilities and rights in addressing the agency and to complain in case they experienced a data protection breach. On the other hand, several others, including participants from Malta, Bulgaria, Germany and Slovakia, expressed misgivings regarding the effectiveness of privacy legislation and also conveyed dissatisfaction with regards to the level of protection offered by the state. These participants argued that privacy breaches are common place, especially where private organizations are concerned. In the main, rather than criticising the legislation per se, participants blamed the lack of action and enforcement by the authorities for such continued and rampant breaches, and consequently argued that the judicial system is rather inefficient in this regard. Moreover, Slovakian and British participants believed that legal safeguards could be circumvented by powerful interests.

On a more general note, in a number of countries, including Austria, Germany and The Netherlands, participants pointed out that the legislation is always a step behind the developments of the fast-moving technological market. Thus it appears that current privacy legislation was considered as being reactive and outdated.

4.4.3 Length of data storage

Expectations regarding ideal length of storage for surveillance data were rather varied in all countries. Some participants appeared to prefer a relatively short storage time ranging from hours to weeks, and argued that a short storage time would minimise the impact on citizen privacy as well as the risk of manipulation of surveillance data. On the other hand, others stated that surveillance data should be stored for months, years or even indefinitely in certain cases. Additionally, some participants appeared indifferent to length of data storage.

In general, it appears that a number of criteria had a bearing on length of data storage, including purpose of use, type of data and locations under surveillance. Some participants argued that unless a crime occurred, surveillance data should be disposed of immediately. In contrast, others argued that surveillance data, even if no incidents are recorded, could be kept for a longer period for any possible use which may arise in the future. Generally participants showed more acceptance towards surveillance data stored for security reasons.

Participants also distinguished between different kinds of data, arguing that storage length should be dependent on type of data. It appears that participants generally favoured longer storage times for data related to criminal acts. In addition, participants also differentiated between the storage of data from sensitive and high-risk locations such as airports and subways, and other safer and less frequented public places.

4.4.4 Data sharing between different actors

In general, participants showed a higher acceptance towards the sharing of data with public authorities than with private organizations since they had more trust in the state. It appears that there was a widespread expectation that private companies would be more likely to misuse data. However, at the same time, participants conveyed concern at the state's position of power with regards to the collection and sharing of citizen data, which could contribute to a growing power imbalance between citizens and state. Moreover, a number of participants appeared alarmed at the thought that their data would be collected and stored in a centralised system, which could be accessible to various state authorities.

5. Conclusion

In all countries, participants displayed high awareness that individual citizens are subjected to surveillance in commercial, boundary and public spaces, as well as when making use of mobile devices. The results indicate that surveillance in these spaces has undergone a process of normalisation, and participants do expect that surveillance occurs in such contexts. While technologically-mediated surveillance was regarded as mostly acceptable for security-related purposes in most spaces, the monitoring conducted in commercial spaces was not always deemed as acceptable by participants. Furthermore, surveillance via the use of mobile devices resulted in feelings of vulnerability for some participants who felt particularly exposed due to the often unknown nature of surveillance occurring through such means. In general, the use of smart surveillance was perceived as more common in sensitive locations, such as airports and public places where mass events take place.

Most participants in all countries believed that massively integrated dataveillance is undoubtedly technically possible. However, the majority of participants were of the opinion that legal restrictions or ethical concerns would prohibit the massive integration of personal data. On the other hand, a minority of participants believed that this practice is already taking place, albeit in a covert manner. Some of the participants believed that the possibility of dataveillance taking place also depends, in part, on individual behaviour as individuals should bear responsibility for divulging their personal information. Integrated dataveillance was generally considered unacceptable as it was believed to pose a threat to citizen privacy. Nevertheless, it appears that acceptance was contingent on several criteria including purpose of use, whether consent was provided, type of data to be collected and shared as well as type of entity – state or private – conducting dataveillance.

Views on the efficiency of smart technologies were rather polarised. While several participants regarded automatized surveillance systems as more efficient in comparison to those requiring a human operator, others were sceptical of technology on its own without human agency. However, the majority of participants agreed upon their preference for a surveillance process which includes a combination of technologically-mediated surveillance and the intervention of human operators.

Participants expressed strong doubts in relation to whether surveillance measures actually provide a viable solution for the reduction or elimination of crime; this belief made it difficult for participants to justify the widespread use of surveillance as they did not equate it with increased security. While most participants acknowledged that the use of technology could be useful for purposes of investigation of crime, at the same time they expressed scepticism with regards to the use of surveillance technologies for the prevention of crime.

In conclusion, intensive surveillance was not only perceived as violating privacy but also as providing a powerful tool to control citizens and to restrict individual freedom. Some participants also pointed out that extensive surveillance could possibly result in the general criminalisation of citizens. In light of this,

most participants argued that extensive surveillance measures could not be justified even in case of escalating crime.

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

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

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

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

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

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

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

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

- ☐ Yes
- ☐ No

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

- ☐ **Yes**
- ☐ **No**

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

- ☐ Yes
- ☐ No

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

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

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

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

	be anonymised before being reported. Hence, the information which will be included in the report will not in any way identify you as a participant. In order to do this, each of you will be assigned a number, and it is this number that will be used in the report. **I also want to make sure that everyone in the group is comfortable enough to share their opinions. To make this possible, I would like to ask everyone present to follow these ground rules:** ▪ **We would like to hear from everyone in the group - we are interested in everyone's opinion** ▪ **There are no right or wrong answers so let us agree to respect each other's opinions** ▪ **Please make sure that your mobile phones are on silent so that the discussion will not get interrupted** ▪ **It is important that comments are made one at a time, since each participant's opinion is important. So let us agree to not speak at the same time, otherwise it will be difficult for us to capture everything that is said during the discussion** ▪ **Let's agree as a group to respect each other's confidentiality so that everyone feels more comfortable in speaking openly.** **If there is anyone who would like to suggest any other ground rules feel free to put your suggestions forward to the group.** **Does anyone have any questions before we start?** **Ok so let me start off by asking you to briefly introduce yourselves to the group without revealing private information. Let's do a round where you tell us your name and maybe something about you. I will start the round myself...** ***(carry out a brief personal introduction)*** ***Running Total: 10 min***

Objectives	Discussion items and exercises
Word association exercise **[About 5mins]** - *Word-association game serving as an ice-breaker* - *Establish top of mind associations with the key themes* - *Start off the group*	***Item 1*** **First up, we will carry out a short game: I will read out a word and I would like you to say the first couple of things that come to mind when you hear the word. Let's try an example first: What is the first thing that comes to mind if I say the word "*food*"? Preferably, try to think about single words or short phrases, avoiding lengthy descriptions.** *Read Out (one at a time):* *Technology, privacy, national security, personal information, personal*

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

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

Presentation of MIMSI scenario to participants

[30mins]

- *To explore participants' understanding of 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...*

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

Aims
1. Participants' first reactions including:

Possibility / impossibility of scenario

1a. How would you feel if this happened to you?
(Also probe to establish the degree of control / helplessness felt by the participants in such a hypothetical scenario)
1b. How would you react if this happened to you? What would you do?
1c. Is such a scenario <u>possible / impossible</u>?

Acceptability / unacceptability of scenario

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

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

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

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

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

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

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

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

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

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

5. Participants'

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

beliefs and attitudes on the benefits and drawbacks of being monitored

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

Running Total: 1 hour 15min

Reactions to scenarios

[About 20mins]

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

Item 5

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

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

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

Variation 1: Even though a significant increase in violent crime is taking place throughout the majority of neighbouring cities, the city you reside in is not experiencing any increase in crime. However the

state still decides to introduce the surveillance measures as a precaution.

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

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 <u>acceptable</u>? Why?
2b. Which technologies do you consider <u>invasive</u> and as a threat to your privacy? Why?
2c. What do you think of these automated (or semi-automated) technolgies whereby the final decision is taken by the system and not by a human operator?

3. Locations of deployment such as:
Airports
Malls
Streets

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

4. Existence of laws and other safeguards

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

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

(in relation to the collection, storage and use of data) *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 – 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 D – CONSENT FORM

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

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date: