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

Noellie Brockdorff[1], Natalie Mundle[1], Christine Garzia[1], Carmen Rodriguez Santos[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Department of Marketing, Universidad de León, León, Spain

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 Spain results of a qualitative study undertaken as part of the SMART project – "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727). The analysis and results are based on a set of three focus group discussions comprising of 28 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 massively integrated dataveillance and the "security versus privacy trade-off".

The Spanish participants were in general highly aware of being under surveillance in different contexts including commercial, boundary and public spaces. Participants mentioned a wide range of surveillance technologies and methods pertaining to different spaces, including the use of CCTV systems and loyalty cards to monitor customer behaviour, financial monitoring, RFID and the deployment of security personnel. Overall, participants perceived customer surveillance in commercial spaces as occurring primarily for security reasons and for marketing purposes. The surveillance of citizens in border spaces and other public areas was perceived as being crucial for reasons of national security and personal safety. Whilst most participants were also aware of the extent of surveillance and its pervasiveness when using a mobile device, some participants appeared rather taken aback by such type of monitoring. In this regard, surveillance was mainly accepted when occurring for reasons of law enforcement, including the prevention and investigation of crime, such as the tracking of criminals.

In order to gauge participants' attitudes and beliefs on integrated dataveillance, the group was presented with a fictional scenario illustrating the massive integration of data. After initial intense reactions to this situation by the majority of participants, the possibility of massively integrated dataveillance occurring was discussed from technical, legal and ethical viewpoints. Even though opinions varied and some participants perceived the scenario as "*surreal*" (P7-III), most considered the massive integration of data as being possible in the near future from a technical point of view. However, from an ethical perspective, most participants perceived the occurrence of dataveillance as unlikely since they found it difficult to conceive that public agencies would engage in such a practice, which was perceived as unlawful by the majority of participants. From a legal viewpoint, participants' opinions were divided: while some expressed their trust in Spanish legislation, others seemed to question its effectiveness.
Participants' opinions on the effectiveness of smart surveillance from a security aspect varied, particularly those in relation to the autonomous decision-making capabilities of smart technologies. When compared to a human operator, automated systems were perceived as more objective and efficient in relation to information processing. These participants believed that automated surveillance systems would safeguard privacy and also lower the risk of manipulation and control. On the other hand, others appeared to be sceptical and distrustful of a surveillance process devoid of human agency.

During the discussion of the “security-privacy trade off” scenario, it appears that some participants showed their readiness of being surveilled for the sake of security, especially when confronted with an increasing level of crime. Notwithstanding, most participants were against renouncing their privacy and freedom for more security. In addition, they were also against extensive surveillance due to the belief that this could result in a power imbalance between citizens and the state.

In relation to different types of surveillance technologies, CCTV in public places was generally considered as acceptable and it appears that the use of video-surveillance has undergone a process of normalisation. Opinions on the effectiveness of ANPR and sound sensors were rather mixed; some participants argued that these technologies are partly ineffective since in the case of ANPR criminals could circumvent surveillance and in relation to sound sensors participants perceived the possibility that incorrect conclusions would be drawn. A rather hostile attitude towards biometric technologies was expressed because of the sensitive nature of the data and the risk of theft and misuse, which resulted in feelings of vulnerability. On the other hand, participants perceived the use of DNA as helpful in crime investigation and the use of electronic tagging as useful for the tracking of criminals.

Participants were also invited to share their viewpoints on surveillance legislation. Opposing views of the effectiveness of legislation were evident; while some participants regarded current legislation as inadequate, others were rather satisfied with the level of protection offered. In relation to the length of storage of surveillance data, expectations were rather varied, however, most participants showed their acceptance for the storage of their data for as long as it was needed for crime investigation.

2. Key Findings

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 Spain is Universidad de Leon (ULE).

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

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

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

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

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research. The focus groups in Spain were carried out on the 23th February, and 13th and 15th March 2013. The composition of the groups held in Spain is described further on in Section 4.

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

3.1 Recruitment process

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

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

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

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

3.2 Discussion guidelines

Discussion guidelines (see Appendix B) were developed with the aim of gauging citizens' awareness and understanding of smart surveillance technologies and also at gaining an in-depth understanding of 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. The Spanish 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 the case of the focus groups held in Spain, the moderators used a video camera to record the discussions. 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 re-categorising and rethinking of the codes first applied, and allowed for a more focussed 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 Spain is based on 28 participants. Although the moderators had no difficulty in recruiting the focus group members, some participants informed the moderators at short notice that they were unable to attend and it proved difficult to replace these participants. In addition, some participants did not show up on the day. It should be noted that this slightly influenced the equal recruitment of male and female participants.

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	M
P2	F	M	F
P3	F	F	M
P4	M	M	No show
P5	M	F	No show
P6	M	M	F
P7	F	F	F
P8	M	M	M
P9	M	M	F
P10	F	No show	F
P11	M	-	-
Total	**11**	**9**	**8**

The atmosphere in all focus groups was described as friendly, free-flowing and cordial, and the moderators had the impression that most participants felt at ease in sharing their opinions. On the other hand, some participants appeared to be slightly intimidated due to the fact that the discussion was being recorded. It seems that some were also intimidated by other group members who appeared to have a good grasp of the topic. In general, participants were described as cooperative and it appears they exhibited great interest and enthusiasm during the discussion.

Focus group 1 (18-25 years) participants were described as very interested in the topic and the discussion was considered as lively. At certain times, participants tended to speak simultaneously, a factor which was said to make the transcription of the interviews slightly more challenging. Due to this, the moderators had to sometimes intervene in order to manage participants' contributions and encourage them to speak in turns. While the majority of participants willingly contributed to the discussion, two participants (P2 and P3) were described as particularly shy. At the end of the focus group discussion, the participants stated that they enjoyed discussing the topic.

As was the case in Group 1, the atmosphere in Group 2 (25-44 years) was also very cordial; however, it was slightly male dominated. The three female participants (P3, P5 and P7) appeared to be either less interested in the topic or else slightly intimidated by the male participants; hence the moderators experienced some difficulty in encouraging them to participate. One participant (P2) was particularly keen on sharing his opinion since he works in a field related to the topic under discussion. Nevertheless, this did not seem to hinder other participants from expressing themselves openly.

The atmosphere in the third and final focus group (45+ years) was described by the moderators as relaxed. The discussion was flowing and the participants were generally cooperative. Although several participants admitted that they felt slightly intimidated by the camera, it appears that this did not influence their contribution to the discussion, with the exception of two participants (P7 and P8). Lastly it was noted by the moderators that this group had a tendency to stray away from the topic and to include rather personal experiences into the discussion; due to this, the moderators had to intervene from time to time to direct the participants' focus back to the discussion topic.

5. Results

5.1 Surveillance Technologies in Different Spaces

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

5.1.1 Commercial Space

In the commercial space, specifically in the context of a supermarket, participants generally displayed a high awareness of the presence of different surveillance devices, including the use of CCTV and loyalty cards: "*The camera is watching you and the loyalty card records what you have bought"* (P4-I).

In all three focus groups, video-surveillance was mentioned as a predominant surveillance measure in commercial spaces. One of the main purposes of CCTV systems was perceived as being theft prevention. Participants expected the establishment to keep the recordings for a limited amount of time before deleting them, so that surveillance data could be forwarded to the police in case of an incident. Additionally, the deployment of security guards and store detectives for the same purpose was frequently mentioned by participants and appeared to be widely accepted. In contrast, the use of security tags on merchandise, which was only mentioned by members of Group 1 (18-24 years), appeared to cause discomfort among participants when passing through the electronic gates at the exit: "*I always feel tense in a supermarket. It does not matter that I have paid, I always think something is going to beep*" (P10-I).

On the other hand, a number of participants argued that surveillance measures were primarily deployed for commercial objectives rather than for the security purposes: "*I think it is more the economic aspect [rather] than security"* (P4-II). In this regard participants perceived the use of loyalty cards as a means to collect client data for the creation of databases which would eventually be sold to third parties. In addition, customer behaviour data was believed to be collected both through loyalty cards and video-surveillance for reasons related to the commercial establishment's marketing strategy: *"The more information they have on people, the easier it is for them to predict how people will behave, and the easier it is to identify ways to sell more"* (P4-I). Generally, the parties involved in the collection of data were identified as being the commercial establishment, the security company and also financial institutions monitoring customer transactions.

In general it appears that these measures were widely accepted both for security reasons and marketing purposes. Lastly, it appears that for most participants, surveillance in this context had no effect on their behaviour, *"I don't notice them or anything. I mean, I go in there and it doesn't even occur to me to look*

and see if there are cameras or not" (P10-III). However, it appears that others felt more aware of being constantly observed in this context: "*They spy on us*" (P8-I).

5.1.2 Boundary Space

In the context of border control, the discussion focused on an airport setting. In this 'boundary space', the focus groups mentioned a wide range of ubiquitous surveillance methods and technologies, including personal data checks, smart CCTV systems with automatic facial recognition (AFR), luggage checks and metal detectors. In addition to technological surveillance, participants also mentioned the presence of security agents and law enforcement officers, as well as the use of sniffer dogs by the latter.

The aforementioned surveillance measures appeared to not only be accepted as necessary but were above all valued for their contribution to national security and passenger safety, most notably in relation to the prevention of crime. Additionally, the collection of surveillance data was believed to be used for the improvement of airlines' marketing strategies. Surveillance was thus perceived as conducted by both state entities, such as the police and customs officers, as well as by private entities, mainly the Spanish Airports and Air Navigation (AENA), who owns and operates the majority of airports in Spain and which was identified by participants as being in charge of the security at airports.

A main source of data collection for security purposes at airports was that related to personal data checks including the examination of passports, identity cards and visas. These documents were regarded as revealing passengers' basic data and as providing a basis for the initial assessment of passengers. In addition to the information obtained through the aforementioned documentation, participants assumed that airport authorities had access to further data about passengers, such as criminal records and bank data, since they expected airports to collaborate and exchange data with different national agencies, including law enforcement agencies: "*I think it is OK that the airport has data but you are not the one who gives it. That is cross-checked with the police*" (P9-II).

Finally, it appeared that some participants from Group 2 (25-44 years) and Group 3 (45+ years) perceived a number of differences between surveillance measures at European airports and in other countries. In particular, Israel was regarded as having extremely strict and intrusive security measures; passengers who had first-hand experience of travelling to this country stated that they felt very uncomfortable being examined in such extensive detail: "*They examine handbags, everything, the whole lot. Even your clothes, it is awful*" (P2-III).

5.1.3 Common Public Spaces

In common public spaces, such as in museums or in stadiums where mass events are organised, participants perceived the occurrence of monitoring primarily for purposes of security and safety. Participants predominantly mentioned CCTV systems and the monitoring of personal data via the

purchase of tickets as main methods of surveillance. To a lesser extent, security checks upon entrance to the venue were also mentioned.

Most participants believed CCTV recordings from mass events to be stored in order to be used for reasons of investigation in case of any incidents: "*Only if something unusual happened then it is examined and if not it is deleted*" (P4-II). It appears that the majority of participants believed these recordings to be stored only temporarily. In relation to the purchase of tickets for events, participants assumed that the collection of data occurred "*not just for the sake of having peoples' data*" (P1-I) but rather for organisational and security reasons, for instance in order to monitor the amount of tickets sold in relation to venue capacity. It appears that participants regarded monitoring measures taken by the police and the government as justified when dealing with large crowds, especially in light of the Madrid Arena tragedy which occurred on the 1st November 2012, where tickets were oversold, thus resulting in mass panic.

With regards to the controls specifically at the entrance of the venue, such as the use of turnstiles and the random frisking of visitors, it appears that surveillance was in this case considered by the participants as a preventive measure by for instance identifying and prohibiting visitors from entering with alcohol or firecrackers.

Lastly, participants also discussed the use of surveillance in other public spaces such as museums. In this context, surveillance measures were seen to be less common than in other spaces; in fact it appears that a number of participants found it difficult to picture how they could be surveilled by this type of institution. Nevertheless, others mentioned the use of CCTV systems and the scanning of visitors' bags for the prevention of vandalism and theft, which was perceived as useful. In general, it appears that participants perceived the aforementioned surveillance measures in the public space as justified, and hence acceptable.

5.1.4 Mobile Devices and Virtual Spaces

In relation to mobile telecommunication devices, Group 1 (18-24 years) and Group 3 (45+ years) participants[2] mentioned two major ways in which surveillance occurs, or can potentially occur, mainly via the recording of conversations and location tracking by GPS. Both monitoring methods were regarded as having a preventive and investigative function in the context of crime:

> "*The police can find out where you are calling from, even when you are calling from a mobile phone, [...] When a crime has occurred, or something, where you were*" *(P9-III).*

In addition to the aforementioned collection of data for reasons of law enforcement, participants also stated that their data would be used by network providers for commercial and marketing purposes.

[2] Surveillance through mobile devices was not address by Group 2 (25-44 years).

More specifically, some mentioned the selling of customer data to mobile phone manufacturers which was believed to be utilised in order to improve the technical capacities of mobile devices.

Overall, it appears that both the recording of conversations and GPS tracking were accepted and considered as necessary by participants in relation to crime-related uses. Nevertheless, a minority of participants showed a lack of awareness and knowledge in relation to the multitude of ways through which surveillance can occur via the use of mobile devices. It appears that these participants expressed not only surprise at the possibility of such monitoring, but also a degree of uncertainty and insecurity about this: "*I do not know, I do not even want to think about it*" (P1-I).

5.2 Perceptions & Attitudes towards Smart Surveillance and Integrated Dataveillance

One of the central tasks of this study was to research citizens' feelings and beliefs towards smart surveillance and massively integrated dataveillance, the latter referring to "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons"[3]. In order to elicit the attitudes of the participants, 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 a range of feelings including extreme discomfort, fear, helplessness and anger. Likened to a *"Big Brother"* (P2-II) scenario in which citizens are spied upon, participants in all focus groups expressed a strong negative reaction: "*Horrible! That is awful*" (P7-I). In general, the idea that this type of extensive surveillance could actually occur resulted in feelings of helplessness: *"[I would feel] frustrated, overwhelmed, I do not know*" (P3-I). Similarly, others stated they would feel resigned to the situation: *"There is nothing you can do"* (P6-II). While overall the majority of participants felt fear and "*panic*" (P7-III), some participants additionally claimed they would feel extremely angry: "*I would be outraged*" (P5-II) and "*pissed off*" (P2-II).

5.2.2 Behavioural Intentions

In addition to asking about participants' feelings upon listening to the hypothetical telephone conversation, participants were also asked for their resulting behavioural intentions. Mirroring the predominant feelings of discomfort and anger as described above, the majority of participants claimed they would engage in a variety of behaviours in order to counteract such a situation. Primarily, these behaviours included pursuing legal action and engaging in self-protection strategies.

In relation to pursuing legal action, participants mentioned a number of behaviours they could possibly engage in. First and foremost, some expressed the necessity to "*report*" (P9-I) the incident since they perceived the massive integration of data as illegal: "*It seems to me that this was done without permission*" (P1-I). Furthermore, focus group 2 participants (25-44 years) claimed they would resort to legal assistance by contacting a lawyer or else by reporting the situation to the Data Protection Agency: "*I would report it. If they really had that information in the system, the agency would send an inspector*" (P2-II). At the same time, however, some participants felt intimidated by the idea of taking legal

[3] Clarke, R. (1997)

[4] The statements of the public servant allude to a drawing together of the job-seekers' personal information from various public and private databases, health-related information, bank / credit card data, surveillance of online social networks, and CCTV.

measures against the state and expressed their doubts as to whether this would indeed be effective. Nevertheless, most participants agreed upon their responsibility as citizens to make use of available "*mechanisms*" (P2-II) in order to defend themselves: "*You can complain and you should complain*" (P6-II).

In relation to self-protection strategies, participants mentioned their own responsibility in protecting their personal data. Participants were particularly aware of the amount of data they themselves revealed in the context of virtual spaces, especially via the use of social networks: "*We are providing this data and more. From the minute we enter into the dynamics of Tuenti, Facebook, Twitter, WhatsApp. [...] They do not stop asking you for information*" (P8-I). Along similar lines, voluntary data sharing which could also be avoided was mentioned in relation to the use of electronic cash cards due to the belief that consumption data could be collected from their use.

5.2.3 Beliefs

5.2.3.1 Likelihood of massively integrated dataveillance

Regarding the likelihood of whether or not smart surveillance and massively integrated dataveillance are possible and realistic (currently and/or in the future), the focus group participants distinguished between technical, ethical and legal aspects. In general, although the development of massively integrated dataveillance was described as "*surreal*" (P7-III) and perceived as "*going too far*" (P2-I), participants did not forgo the possibility that dataveillance could occur: *"[It is] unlikely but I do not think it is impossible*" (P6-II). In addition, a number of participants seemed to assume that dataveillance was already widespread in their everyday lives.

From a technical point of view, participants believed that the rapid development of surveillance technologies could eventually lead to extensive dataveillance: "*The way technology is advancing, I think it will [become reality]*" (P3-III). In spite of this, however, participants appeared sceptical that the massive integration of data would actually occur in their own country: "*It is technically possible, but in Spain it is very unlikely* (P4-II); however they did not specify the reasons for this belief.

The likelihood of occurrence of massively integrated dataveillance was also considered as depending on the entities involved. Here the participants appeared to distinguish between private organisations and public entities. In particular, it seems that they found difficulty in envisaging the involvement of a public agency in illegal data collection and sharing: "*If it is a public service, I do not think [it is possible]*" (P1-III), while in the case of private entities this was perceived as more possible.

Moreover, although opinions were rather divided, the majority of participants expressed their trust into Spanish legislation, which they regarded as providing a suitable protective mechanism: "*The legislators would not allow it. In fact, Spain is one of the most restrictive countries in terms of privacy issues*" (P2-II). Participants seemed to have faith that a shift in attitudes at a societal level was occurring: "*I think we*

are moving closer and closer to the idea that 'privacy is paramount'" (P8-II). Nevertheless, other participants feared the unpredictability of future developments of legal frameworks and therefore did not exclude the possibility of dataveillance to become legal: "*Conditions may change*" (P1-II).

5.2.3.2 Acceptance of massively integrated dataveillance

Overall, it appears that the acceptance level of most participants towards massively integrated dataveillance was rather low and that participants were principally against extensive dataveillance, mostly since this was perceived as presenting an invasion of privacy: "*People's privacy should not be controlled so much*" (P3-III). The notion of control was a major reason for most participants to reject surveillance, and it appears that they felt insecure not knowing who possessed their data. This power imbalance between the state and its citizens was perceived as providing an opportunity to manipulate the lives and activities of citizens: "*In theory the police have all the data of an individual, [...] and they are supposed to work in our best interest, but […]*" (P2-II).

A further concern expressed by some focus group members 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. This collection and sharing of identifiable personal traits was not only seen as a threat to peoples' privacy and freedom, but also as providing opportunities for the manipulation and control of citizens : "*In the end, your life is not your own anymore*" (P1-II).

With regards to the collection of data by state authorities, such as the employment agency, participants pointed out at the absurdity of allowing civil servants easy access to such an extensive amount of private information: "*You want to find some work and some bloke comes along and says I am going to inquire [about] your past*" (P10-I). Consequently, it appears that an important factor influencing acceptability was perceived purpose and necessity of data collection:

> *"Sometimes you go to do an administrative procedure and they ask you for your address, ID number, name and surname, date of birth. Information that is often not necessary at all. What on earth does it matter to the doctor, when you fill out paperwork, where you live?" (P9-II)*

Nevertheless, when it came to issues of security, some participants expressed their trust into the use of surveillance with the aim of ensuring or increasing security: "*I think that it is fine as far as security is concerned but not for control*" (P1-II). Therefore, many participants tolerated the collection of data by law enforcement agencies especially in relation to crime prevention and investigation: "*Really, [they can collect] anything that has to do with security*" (P4-I).

Participants also discussed the type of personal data which they considered acceptable or unacceptable to share. It appears that most participants felt uncomfortable about sharing more than their basic data. Overall, information relating to personal relationship status, bank and medical data appeared to be unacceptable to share. Here the participants expressed their concern about the spreading of these

details in the public sphere: "*It scares me that they have my medical records for example. It should not be in the public domain*" (P6-III).

Lastly, in contrast to the above, a minority of participants appeared unconcerned by extensive dataveillance from a privacy aspect. These participants seemingly believed that as long as one has nothing to hide, there is no reason to be worried about one's publicly accessible data: "*I do not think that would bother me. It seems that an open book, once it is open, it has nothing else to hide. So I think that I would not be afraid*" (P10-III).

5.2.3.3 Perceived effectiveness of smart technologies and integrated dataveillance

When discussing the effectiveness of surveillance technologies, participants differentiated between more traditional technologies, in which case it was perceived that human judgement is necessary in decision-making, and smart technologies, in which case it was perceived that decisions are taken by a computer programme. The issue of automation brought up mixed feelings amongst participants, and the main issue of discussion was the difference in the perceived effectiveness of a decision taken by a human or a machine and its impact on citizens' privacy.

When it came to issues of privacy, most participants seemingly perceived automation as less intrusive: "*So if you tell me Google is storing information automatically, at least I feel safer than if a person, a human being, was looking at my information*" (P9-II). In addition to privacy reasons, participants perceived the presence of human operators as presenting a possible risk; for instance it was mentioned that operators could intentionally misuse or manipulate surveillance technologies for their own purposes, such as stalking: "*A camera cannot follow you, but a person can*" (P1-I). In general, participants seemed uneasy at the lack of supervision of human operators: "*But who monitors the person who is behind the camera [...]?"* (P2-I)

With regards to the reliability of surveillance measures, most participants perceived the decision-making process by a machine as "*more logical and more neutral*" (P3-III) than human decision-making. Unlike machines, human operators were considered easily influenced by their biases, an aspect which was perceived as possibly contributing to an inaccurate assessment:

> "*I would almost trust machines more than I would humans, because machines would just go about what they had to do, whereas humans maybe they might see, or want to see, or see what they wanted*" *(P10-III).*

However, this point of view was challenged by some participants who stated that a machine was after all programmed by a human. Here it was argued that humans could possibly transfer their biases to the machine through the programming process or even purposely manipulate the technology, which would put the perceived neutrality of technology into question:

"*Who programmes the system and says that this is right or this is wrong? This is dangerous, isn't it? In the end that is decided by a person, it does not depend on a machine*" *(P3-I).*

Furthermore, most participants questioned the accuracy of surveillance technologies in differentiating between ambiguous situations. Moreover, although machines were regarded as efficient vis-à-vis the processing of information, a final decision by a human operator was considered necessary in order to guarantee a correct decision: "*Machines can process the information, but they should not be the ones that decide because they are incapable of reasoning*" (P9-II).

Lastly, another issue in relation to effectiveness of surveillance was the belief that in cases of crime investigation, the identification of criminals with the use of smart technologies was problematic and ineffective due to the belief that criminals could circumvent their identification by changing their physical appearance: "*Camera recordings cannot tell us everything. If you have covered yourself, pulled something over you, [you can] shoot someone twice and leave*" (P8-I). Similarly, the possible identification of criminals via biometric data such as DNA and fingerprints was considered as extremely difficult: "*These days [criminals] cover their fingerprints with paraffin when they go to steal. Not to mention gloves which makes it impossible to detect fingerprints*" (P3-III).

5.3 Security – Privacy Trade-Offs

5.3.1 Acceptance of Technological Surveillance

In order to gauge participants' perceptions vis-à-vis the security-privacy trade off, as well as their attitudes towards a number of specific smart technologies, a hypothetical scenario was presented to the group. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging 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, participants' reactions were somewhat varied, although a general pattern could be distinguished. Overall, only a minority of participants found the measures in this particular context as acceptable, particularly when their personal safety was perceived to be under threat: "*If you are afraid that when you go out they [criminals] will do something to you, well, I think that [surveillance technologies] are fine*" (P10-III). In relation to this, a difference between attitudes was noted between groups since most of the participants who found the measures acceptable were from Group 3 (45+ years). In contrast, the majority of participants belonging to Group 1 (18-24 years) and Group 2 (25-44 years) and a minority of participants from Group 3 (45+ years) objected to the use of surveillance measures even in case of an increase in crime; it appears that the participants rejected the notion of having to compromise their privacy for more security: "*You have to give up so much privacy to be safe. That is what is left of your privacy...bah!*" (P4-I)

The vulnerability and insecurity of participants with regards to smart surveillance appeared to stem from different factors. Firstly, an aspect which emerged strongly during the discussion of the scenario was the ethical dimension. A major criticism of extensive and incessant surveillance was not solely related to privacy violations but also to the impact of surveillance on liberty rights. The majority of participants considered their privacy as being "*fundamental*" (P4-II) and more important than security, especially since they perceived the surveillance measures in the scenario as being "*out of proportion*" (P2-II) and "*over the top*" (P9-II). In their opinion, it was impossible to achieve, and maintain, a balance between security and privacy since the extent of privacy to be sacrificed was too high in comparison to the minor gains in security achieved with the use of surveillance: "*What I gain in security, I lose in privacy. I mean, for all the privacy I lose, I gain a little bit of security, but overall I gain less*" (P4-I).

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

In line with the above-mentioned reservations, a number of participants doubted and challenged the notion that surveillance was the best solution to reduce or eliminate crime. In their opinion, the use of surveillance did not provide a deterrent effect for criminals with clear intentions: "*If someone wants to kill you, there are going to do it whether there is a camera, a sensor […]"* (P1-I). Furthermore, participants argued that the intensification of surveillance in society was based on mistrust; this was perceived as resulting in a general 'criminalisation' of citizens in spite of their innocence: "*If the town's citizens have not done anything, why do you have to go and distrust them?*" (P5-I) In response to this lack of trust in citizens, the participants questioned their own trust of state surveillance: "*Why should I trust them when they do not trust me*?" (P1-I) and proceeded to argue that effort should be directed towards the development of knowledge and moral values in society: "*The key to this is education*" (P1-I).

Furthermore, several participants perceived that the introduction of surveillance and dataveillance tools by the state could potentially be employed for the unjustified monitoring of citizens. They argued that in this case, security could possibly be used as a pretext to disguise such hidden agendas: "*It is like using security as an excuse to collect your information, often without your consent*" (P4-II). It appears that the ambiguity surrounding motivations for surveillance resulted in a heightened level of insecurity: *"At the same time that they are trying to offer me security, they are taking it away from me*" (P2-I).

The second major reason as to why the extensive use of smart surveillance as described in the hypothetical scenario was considered as generally unacceptable was the anxiety caused by the perceived threat of misuse of citizens' data and the risk of corruption, both of which were regarded as realistic threats:

> "*So we do not know what they might do with that information. Almost everyone has a price, so if someone wants to know something about you, they only need to go to the person behind [the surveillance] who has access to the information in order to find out everything about you*" *(P8-I).*

In light of this, participants appeared concerned and raised the issue of who is monitoring those who are actually surveilling others: "*I would feel vulnerable because [...] the people who have all that information about me, who watches over them*?" (P2-I)
Nevertheless, a number of participants appeared to tolerate the discomfort of being surveilled as long as crime was prevented and citizen protection increased: "*If you want more security you have to give more [information] because they do not know if you are good or you are bad*" (P4-I). For some participants surveillance measures appeared to be acceptable as long as such tools are employed solely for security-related purposes with no hidden agendas: "*As long as it is for a purpose and not to take advantage of you*" (P9-I). It appears that a number of participants believed in the efficiency of surveillance in combating crime and were keen to point out the advantages of surveillance: "*Something could happen at any moment and then you are prepared*" (P10-III). In addition, they found it reassuring that law enforcement agencies would have access to their data: "*I think it is a very good thing that the police have information*" (P1-III).

Nevertheless, when participants were confronted with a significantly increasing crime rate in the alternative versions of the original scenario, most participants did not significantly change their opinion, except for the minority of participants mentioned previously. These participants considered an increase in criminality as a realistic threat, and such circumstances were regarded as conducive to increased tolerance of surveillance measures and a corresponding readiness to compromise citizen privacy: "*It is a chain that begins with stealing [something] from one person, but ends with killing many*" (P1-III). Moreover, some participants also pointed out that while it is relatively easy to reject surveillance measures when not directly affected by crime, attitudes towards surveillance can shift in cases where one is personally affected:

> *"You get to a point where you say "bah, not me, it wouldn't affect me […]" But if it does happen to you, if it's your family, you would think that there ought to be more vigilance" (P9-I).*

With regards to the locations of deployment of surveillance devices, participants accepted their use in public spaces which experience large flows or masses of people, such as streets, town centres, subways and shopping centres, and in places considered as high risk areas, such as banks and airports. Nevertheless, there was a minority of participants who did object to constant monitoring in public spaces: "*You have got a 24-hour police officer. It is like sleeping next to the walls of the police station*" (P9-II). Furthermore, surveillance in private spaces was considered as unacceptable by most participants because it was perceived not only as a violation of privacy but also as impinging on one's freedom:

> "*I think that monitoring 100% of your time is intolerable. Monitoring at a given time in a particular place is okay, but people need to have privacy in their lives or at home. [There] they need to know that no one is watching or monitoring them. Otherwise, I think that goes against the freedom of the individual" (P4-II).*

5.3.2 Perceptions of Different Technologies

In general, different types of surveillance technologies appeared to meet different levels of acceptance. Firstly, it seems that acceptance was primarily contingent on context of use, and in this regard, it appears that participants found difficulty in understanding how ANPR, sound sensors, the use of fingerprints and electronic tagging of vulnerable groups could be used in order to contribute to public order and citizen safety. As mentioned previously, while most of the members from Group 3 (45+ years) appeared to tolerate most surveillance technologies for the sake of security, the other participants appeared to perceive most measures as extremely intrusive and exaggerated.

Overall, while CCTV appeared to be generally accepted and even desirable for security purposes, the function of automatic face recognition (AFR) was perceived by many participants as breaching citizens' privacy. Despite considering sound sensors as acceptable, at the same time participants regarded this type of technology as rather inefficient. Biometric technologies and electronic tagging provoked a strong

reaction amongst group 1 (18-24 years) and group 2 participants (25-44 years), who specifically regarded electronic tagging as "*the most invasive of all [technologies]*" (P4-II).

The use of CCTV systems appeared to have gone through a process of normalisation and seemed to be widely perceived as "*acceptable"* (P2-II) as long as it was not applied in an unlimited manner and as a "*blanket measure*" (P4-II). Moreover, participants argued that unless citizens committed illegalities, there was no need to be apprehensive at being under surveillance. In general, the use of traditional video-surveillance appeared to enhance participants' feelings of personal safety, especially in public areas. However, this contrasted sharply with the feelings provoked by the function of AFR; in this case it appears that the integration of databases and the possibility of being identified caused some participants to feel that *"there is no escape*" (P1-I).

With regards to ANPR, some participants regarded the technology as useful and acceptable when it was used for electronic toll collection. However, it appeared to be perceived as ineffective for speed limit enforcement due to the drivers' possible awareness of the location of the technology, which would allow them to avoid detection by temporarily slowing down their speed to the speed limit: "*You just brake and carry on*" (P3-I).

The use of sound sensors was subject to mixed reactions. On the one hand, some participants found them acceptable for the recognition of screams and noises, perceiving them an efficient security measure in relation to intervention. On the other hand 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 to make their point.

In contrast to the aforementioned technologies, biometric surveillance and electronic tagging seemed to provoke a heightened sense of vulnerability among the majority of participants, who appeared particularly concerned about the possible risk of DNA theft and its consequent misuse by criminals at a crime scene: "*They [the criminals] could take your DNA and place [your traces] there and that's it*" (P5-I). In light of this, most participants agreed upon the collection of DNA data exclusively for criminals, as opposed to the indiscriminate collection of DNA from all citizens:

> "*If it is [collected from] everyone, that does seem invasive to me. If it is only those who have already done something, then it seems okay to me […] in that case, nothing is going to happen to the person who has not done anything*" *(P4-I).*

Another reason for rejecting the use of DNA data for surveillance purposes was due to the link between DNA and health data, which was considered as extremely sensitive information. Nevertheless, participants also mentioned that for the investigation of crimes, it would be practical to have all citizens' registered, because otherwise a first-time criminal could not be identified:

> "*I do not want them to have my DNA, but the day after tomorrow if my brother was killed and they found a hair on his pillow from someone else, until they have the DNA of that person they cannot identify whose hair it is. Well, I would be wishing that they had the whole world's DNA to arrest his murderer*" (P1-I).

In relation to the use of electronic tagging and chips, their use was considered as "*great*" (P1-I) by some participants when deployed exclusively for criminals. This technology was also considered useful for elderly suffering from memory loss or conditions such as Alzheimer's disease. However, such use was considered as acceptable on condition that it was voluntary and that the supervision was not carried out by the state but by the person's family. Nevertheless, in other circumstances, the constant control of individuals was considered as an invasion of privacy and was strongly rejected by many participants. This was especially so in relation to the supervision of children, since the use of such control was perceived as a wrong approach to adopt: "*If we make children wear bracelets to track them, it is a step backwards. They will not learn to pay attention. […] To me it is the same as putting them on a leash*" (P2-I).

5.4 Surveillance Laws and Regulations

During the last part of the focus group sessions, issues relating to surveillance laws and regulations were discussed, including effectiveness of surveillance laws and regulations, participants' level of trust in the state, length of data storage and issues of data sharing between different entities.

5.4.1 Trust in the state and effectiveness of legislation

Participants were asked about their views on privacy legislation and opinions were somewhat divided on the effectiveness of, and protection offered by the legislation. Firstly, some participants believed that privacy legislation does offer a protective mechanism:

> "*'Protected' might not be the right word, but at least we have an instrument to fall back on if something happens […] The system might not be perfect, but hey, at least it is there. In other countries there is nothing*" *(P2-II).*

On the other hand, others expressed their dissatisfaction with regards to the level of protection offered by the state. These participants argued that privacy breaches are commonplace, which they blamed on a lack of sufficient enforcement rather than on the legislation per se: "*The laws are wonderful, [but] then the problem is the compliance with them*" (P1-III). As a result, participants perceived a loss of control and a lack of protection over their data: "*In the end you come to realise that they can do whatever they want with your data*" (P3-I).

Nevertheless, Group 2 members (25-44 years) showed their trust into the functioning of the state's Data Protection Agency and referred to citizens' responsibility, and right, to address the agency and to complain in case they experienced a data protection breach:

> "*There has to be a complaint. If not, nothing happens. […] The agency is not like a police force going around. [But] if you lodge a complaint, they are obliged to act and to investigate what happened*" *(P2-II).*

5.4.2 Length of data storage and accessibility

Participants were also asked about their opinions on length of storage for surveillance data, which was particularly discussed at length by group 2 (25-44 years). A number of criteria were mentioned, including purpose of data collection and the entity having access to the data. In the first place, it appears that a number of participants stated their acceptance of data stored for security reasons. Secondly, in relation to data access, some participants stated they would not be concerned about length of storage if this was accessed solely by law enforcement agencies. Nevertheless, in contrast to the latter, others were convinced that a minimum storage time was essential in order to minimise the impact on citizen privacy

and possible risk of manipulation. It appeared that the longer data was stored, the higher the threat of misuse was perceived to be: "*The chances that more people will have access to it are greater, the longer the information is stored […] they are people and they could use it for something else*" (P9-II). Moreover, participants expressed concern that a change in political direction could lead to changes in legislation with unknown consequences: *"If at a given time the winds blow in another direction […] who can guarantee that it [the data] will be used correctly?"* (P4-II) Therefore, a definite storage time appeared to be perceived as necessary in order to protect citizens' data from unexpected future events.

When asked to propose a specific time frame for the storage of data, most participants appeared to find difficulty in specifying what they would consider as an ideal period. In general, opinions varied considerably and ranged from storage times lasting days, weeks or months, with some also suggesting that this data should be kept till the death of the person concerned. In the case of a definite time range, participants agreed upon the deletion of their data after this timeframe expired and in case that no criminal event is recorded: "*There comes a point when, if nothing has happened, there is no reason for anyone to have your information*" (P9-II). Nevertheless, with regards to criminals, most participants agreed that their data, in particular DNA, should be kept for longer, even for *"all their lives"* (P1-I) because in their opinion *"if a person is a murderer, he will always be"* (P1-I).

5.4.3 Data sharing between different actors

In general, participants showed a higher acceptance towards the sharing of data with public authorities rather than with private ones since they had more trust in the state: "*I would prefer that [my data] was in public hands rather than in private [hands]. The state is supposed, in principle, to look out for its citizens […]*" (P4-II). It appears that there was a widespread expectation that private companies would be more likely to misuse data.

However, at the same time, participants feared the state's position of power with regards to the data collection and sharing of citizen data: "*The state can do what it likes and does not have to be accountable to anyone, but regarding a private company, you have to agree to sign a contract*" (P6-I). In addition, some participants expressed concern that the ever increasing collection and sharing of citizen data could "*give the authorities a lot of power"* (P2-II) and thus 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 they perceived would be accessible to all state authorities *"[…] the day will come when there will probably only be one file, so to speak, and then everyone has that information"* (P2-II).

With regards to the sharing of personal information with private actors, some participants mentioned the case of job applications. These participants argued that most people spontaneously divulge certain data, such as nationality, which would not necessarily be needed by the employer, although the latter would have asked for this information. While discussing this example, participants appeared to criticise

citizens' lack of questioning in relation to data sharing, which, in their opinion, derived from a normalisation process: "*We are already used to give this information*" (P2-II).

6. Conclusion

Throughout the different focus groups, the Spanish participants indicated a generally high awareness that individual citizens are indeed the subjects of surveillance in the main spaces considered during the discussion. In general, it appears that surveillance by CCTV in public and border spaces has undergone a process of normalisation and acceptance for security-related purposes. In commercial and virtual spaces, participants considered massively integrated dataveillance as generally acceptable for the prevention and investigation of crimes, including the tracking of criminals. Nevertheless, some participants expressed surprise upon learning about the ways in which surveillance can occur through mobile phones.

For most participants, extensive dataveillance by the state was seen as unacceptable and a number of participants appeared to believe that it was their responsibility to stand up for their rights and to defend their privacy. Nevertheless, due to the quick pace of technological progress, the development of dataveillance was deemed as likely; however, participants appeared to believe that existing legislation adequately protected citizens' privacy rights.

With regards to the acceptance of massively integrated dataveillance, many participants showed their fear of being controlled and manipulated by a state with unrestricted access to one's private data, which was seen to result in a power imbalance. However, surveillance and massively integrated dataveillance were also accepted for crime investigation, prevention and an increase in the general security.

Overall, a number of participants expressed a lack of trust in relation to the operational nature of smart technologies and their automatic decision-making process, expressing doubts at the ability of machines to differentiate ambiguous situations, which could possibly result in misinterpretations and erroneous conclusions. On the other hand, the decision-making process of automated systems was perceived as more efficient and objective. The use of smart surveillance was also perceived as reducing the risk of corruption and manipulation of data, and as safeguarding privacy by some participants.

Further main concerns which emerged in relation to surveillance were the risk of an unjustified monitoring of citizens, a general criminalisation of citizens and the resulting development of mistrust in society. In addition, doubts were raised by most participants in relation to whether surveillance measures actually provide a viable solution for the reduction or deterrence of crime, which made it difficult for participants to accept being monitored. Nevertheless, a number of participants were willing to sacrifice their privacy to a certain extent for the sake of increased safety in a context of escalating criminality.

With regards to the acceptance of different technologies, it appears that technological surveillance was mainly accepted with regards to the use of CCTV in public places, because it made participants feel safer. It also appears that video-surveillance has gone through a process of normalisation. In contrast, the effectiveness of ANPR and sound sensors was questioned since some believed that criminals could

circumvent these technologies. Additionally, the risk that the use of sound sensors results in wrong conclusions being made was considered as high. A rather hostile attitude towards the use of biometric data was expressed because of the sensitive character of the data and also due to the risk that this data could be stolen or misused, which made participants feel extremely vulnerable. On the other hand, participants perceived the use of DNA as helpful in crime clarification, and the use of electronic tagging was considered as acceptable for the tracking of criminals and elderly people at particular risk of going missing.

In relation to legal protection, although participants perceived the existing legal framework as providing sufficient protection for citizens, participants believed that legislation needed enforcement in order to be efficient. Lastly, with regards to surveillance data storage, participants felt that data should be stored for the amount of time needed for crimes to be solved.

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

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

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

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

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

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

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

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

- ☐ Yes
- ☐ No

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

- ☐ **Yes**
- ☐ **No**

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

- ☐ Yes
- ☐ No

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

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

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

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

	participant. In order to do this, each of you will be assigned a number, and it is this number that will be used in the report. **I also want to make sure that everyone in the group is comfortable enough to share their opinions. To make this possible, I would like to ask everyone present to follow these ground rules:** ▪ **We would like to hear from everyone in the group - we are interested in everyone's opinion** ▪ **There are no right or wrong answers so let us agree to respect each other's opinions** ▪ **Please make sure that your mobile phones are on silent so that the discussion will not get interrupted** ▪ **It is important that comments are made one at a time, since each participant's opinion is important. So let us agree to not speak at the same time, otherwise it will be difficult for us to capture everything that is said during the discussion** ▪ **Let's agree as a group to respect each other's confidentiality so that everyone feels more comfortable in speaking openly.** **If there is anyone who would like to suggest any other ground rules feel free to put your suggestions forward to the group.** **Does anyone have any questions before we start?** **Ok so let me start off by asking you to briefly introduce yourselves to the group without revealing private information. Let's do a round where you tell us your name and maybe something about you. I will start the round myself... *(carry out a brief personal introduction)*** *Running Total: 10 mi*
Objectives	**Discussion items and exercises**
Word association exercise **[About 5mins]** - *Word-association game serving as an ice-breaker* - *Establish top of mind associations with the key themes* - *Start off the group*	***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 many roles*	*For each item, and where relevant, probe in detail to explore the following:* 1. ***How is the information being collected:*** a. ***Which types of technologies do you think are used to collect your personal information?*** 2. ***What type of information is being collected:*** a. ***What type of personal information do you think is being collected?***

3. Explore the participants' understanding of where their information is ending up *4. Explore the participants' views as to 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*	***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***

MIMSI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Aims

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

1. Participants' first reactions including:
- Possibility / impossibility of scenario
- Acceptability / unacceptability 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 possible / impossible?
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 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*

Aims:

1. Security climate and level of threat

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 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":

1a. What makes you feel safe 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 (in relation to the collection, storage and use of data)

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>?

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 <u>acceptable timeframe</u>?

	Running Total: 1 hour 35min
Brief summary of discussion [5mins] ▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***Item 6 – Summing up session*** ***At the end of the focus group, it is helpful to provide a summary of the emerging points. Here you should aim at giving a brief summing up of the themes and issues raised during the discussion. After, you can ask for the following from the participants:*** - ***"How well does that capture what was said here today?"*** - ***"Is there anything we have missed?"*** - ***"Did we cover everything?"*** ***This brief session will give participants an additional opportunity to express their views and can also be used to elaborate on topics raised but not pursued at the time.*** ***Running Total: 1 hour 40 min***
Conclusion of focus group **[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 (SPANISH)

Introducción	Sesión informativa
Bienvenida a los participantes - *Saludo a los participantes* - *Reparto de tarjetas identificativas* - *Firma de los formularios de consentimiento*	*Reciba a los participantes tan pronto como lleguen. Asigneles un asiento y proporcioneles una tarjeta identificativa.* *Distribuya el formulario de consentimiento a los participantes y pidales que lean y firmen el formulario antes de comenzar el grupo de referencia. Esto es importante para asegurar que los participantes entiendan lo que han aceptado hacer.*
Introducción aprox.10 min] - *Gracias* - *Introducción del equipo facilitador* - *Propósito* - *Confidencialidad* - *Duración* - *Regas de juego para los participantes* - *Breve presentación de los participantes*	**Bienvenidos a este grupo de referemcia y gracias por aceptar participar en esta sesión. Les agradecemos que hayan reservado este tiempo de su apretada agenda para participar en este proyecto, por lo que valoramos mucho su presencia.** **Mi nombre es _____ y voy a llevar a cabo el debate en grupo. Voy a ser ayudado por _____ mi co-moderador, que estará tomando notas y grabando nuestra conversación.** *Presentar ar cualquier otro compañero que también pueda estar presente* **La sesión dura entre una hora y media y dos horas y ya que estaremos grabando en video el debate, yo amablemente les pido que hablen en voz clara. Sus opiniones y pensamientos son muy importantes para esta investigación, y no queremos perder ninguno de sus comentarios.** **Tal y como se les informó cuando fueron contactados para participar en este debate, este grupo se centra en el tema de la tecnología y la privacidad, y se lleva a cabo como parte del Proyecto SMART, que está co-financiado por la Unión Europea. Aquellos de ustedes que deseen saber más sobre el proyecto SMART, por favor hágannoslo saber y procederemos a darles más información cuando finalicemos el grupo de enfoque.** *En este momento es importante no divulgar ningún detalle adicional sobre el contenido del grupo de enfoque con el fin de evitar la influencia y polarización del debate posterior.* **Como les informamos al leer y firmar el formulario de consentimiento, todo lo que se grabará durante esta sesión será confidencial y su identidad permanecerá en el anonimato. Esto significa que sus comentarios serán compartidos sólo con quienes participan en este estudio y se utilizarán en publicaciones científicas relacionadas, y se harán anónimos antes de que consten en los**

	informes Por lo tanto, la información que se incluirá en ellos no les identificará de manera alguna como participantes. Para hacer esto, a cada uno de ustedes se le asignará un número, que posteriomente se utilizará en el informe. **También quiero asegurarme de que todos en el grupo estén lo suficientemente cómodos como para compartir sus opiniones. Para hacer esto posible, me gustaría pedir a todos los presentes que sigan estas reglas básicas:** **Nos gustaría escuchar a todas las personas del grupo. Nos interesa la opinión de todos.** **No hay respuestas correctas o incorrectas, así que acordemos respetar las opiniones de los demás.** **Por favor, asegúrese de que los teléfonos móviles están en silencio para que el debate no se interrumpa.** **Es importante que los comentarios se hagan de uno en uno, ya que la opinión de cada participante es importante. Así que pongámonos de acuerdo para no hablar al mismo tiempo, ya que de lo contrario nos será difícil captar todo lo que se dijo durante el debate.** **Pongámonos de acuerdo como grupo en respetar la confidencialidad de cada uno, para que todos se sientan más cómodos a la hora de hablar abiertamente.** **Si hay alguien a quien le gustaría sugerir otras reglas básicas, no dude en exponer sus sugerencias al grupo.** **¿Alguien tiene alguna pregunta antes de comenzar?** **Muy bien, permítanme en primer lugar pedirles que se presenten brevemente al grupo sin revelar información privada. Vamos a hacer una ronda en la que cada uno diga su nombre y tal vez algo sobre uno mismo. Voy a empezar la ronda por mí ...** ***(Realizar una breve presentación personal)*** *Tiempo Total: 10 min*
Objetivos	**Puntos de Debate y Ejercicios**
Ejercicio de asociación de palabras **[Aprox. 5 mins]** - *Juego de asociación de palabras para cortar el hielo* - *Establecer las*	***Item 1*** **Para comenzar vamos a jugar a un pequeño juego: Yo leeré en voz alta una palabra y me gustaría que ustedes dijesen el primer par de cosas que les vienen a la cabeza cuando escuchan dicha palabra. Vamos a probar primero con un ejemplo: ¿Qué es lo primero que le viene a la cabeza cuando digo la palabra "comida"? En lo posible, traten de pensar en palabras sueltas o frases cortas, evitando descripciones complicadas**

asociaciones principales con los temas claves. - *Comenzar el debate en grupo*	*Leer en voz alta (de una en una):* *Tecnologia, privacidad, seguridad nacionalinformacion personal, seguridad personal* *Tiempo Total: 15min*
Debate sobre la vigilancia en situaciones cotidianas **[20 min]** - *Para explorar la experiencia de los participantes con la vigilancia y cómo la perciben.* - *Para explorar el conocimiento y si los participantes se han percatado de las diferentes tecnologías de vigilancia* *Objetivos:* *1. Explorar la conciencia y los conocimientos de los participantes sobre las tecnologías* *2. Explorar la*	***Item 2*** **Vamos a hablar de otra cosa. Quiero que piensen en los casos en los que sienten que ustedes o sus acciones están siendo observadas, así como cualquier momento en el que son conscientes de que su información está siendo recopilada. Vamos a empezar por pensar en actividades que generalmente realizan en su vida cotidiana. Tomemos las siguientes situaciones como ejemplos** **Escenario 1: Supermercado** **Como primer ejemplo podemos tomar el ir de compras a su supermercado habitual. ¿Pueden compartir sus pensamientos sobre esto?** **Escenario 2: Viajar** **Vamos a pasar a otra situación, esta vez relacionada con los viajes. ¿Qué pasa cuando viajan en avión?** **Escenario 3: Lugar público (por ejemplo, un museo, un estadio)** **Ahora imaginen que están visitando un lugar público, como un museo o asistiendo a un evento como un partido de deporte o un concierto. ¿Qué tipo de actividades cree usted que serían registradas/controladas?** **Escenario 4: Dispositivos móviles** **Vamos a debatir únicamente un último ejemplo. Piensen en las veces que usan su teléfono móvil. ¿Qué creen que se está grabando en ese caso?** *Para cada item, siempre que sea pertinente, pruebe a explorar en detalle lo siguiente:* ***1. ¿Cómo está siendo recopilada la información?:*** ***a. ¿Qué tipos de tecnologías creen que se utilizan para recoger su información personal?*** ***2. ¿Qué tipo de información esta siendo recogida?***

experiencia de los participantes al sercontrolados en susdistintos papeles

3. Explorar el conocimiento de los participantes sobre hasta donde llega su información

4. Explorar las opiniones de los participantes sobre por qué sus acciones y comportamientos son observados, controlados y recogidos.

b. Qué tipo de información personal piensan que está siendo recopilada?

3. ¿Quién está recopilando la información?

a. ¿Quién piensan que es responsable de recopilar y grabar su información personal?

b. ¿Dónde creen que acabará su información personal?

4. ¿Por qué esta siendo recopilada, grabada y almacenada la infromación?

a. ¿Por qué piensan que su información personal está siendo grabada y recopilada?

b. ¿De qué forma piensan que será utilizada su información personal?

Tiempo Total: 35min

Presentación de tarjetas que representan diferentes tecnologías y aplicaciones [10 mins]

Para exponer a los participantes a una selección de tecnologías y aplicaciones inteligentes relevantes, con el fin de permitir una mejor comprensión y por lo tanto para facilitar la discusión

Item3

Presentar al grupo las siguientes tres cartas (cada una representa un grupo de diferentes tecnologías y aplicaciones). Las tarjetas incluirán las descripciones siguientes:

Tarjeta 1 – tecnologías de Reconocimiento y seguimiento de personas o eventos: *Circuito Cerrado de Televisión de Movimiento Automático (CCTV), Lector Automático del número de matrícula (ANPR) o identificación automática del número de matrícula de los vehículos (AVNI), y dispositivos de rastreo como el seguimiento de teléfono móvil y RFID*

Tarjeta 2 - Biometría: *Tecnologías biométricas como el escaneo de las huellas dactilares y el iris y el reconocimiento facial automático (AFR)*

Tarjeta 3 - Dispositivos de detección de objetos y productos: *Arco detector de metales (portal) y dispositivos de rayos- X*

Tiempo total: 40min

Presentación del escenario MIMSI a los participantes [30 mins]

- *- Explorar la comprensión de los participantes sobre las implicaciones de MIMSI*
- *Explorar los sentimientos, creencias y actitudes de los participantes frente a **u**n vis a vis de intercambio de información personal*

Item 4

Presente la siguiente situación hipotética al grupo. Se puede preparar de antemano una grabación de la conversación telefónica y presentarla al grupo.

Conversación telefónica con el agente de atención al cliente en la oficina principal del Servicio Público de Empleo

***Agente de Atención al Cliente**: Buenos días, le atiende Sharon, Cómo está usted Sr. Brown? Hemos estado esperando su llamada puesto que su contrato de trabajo finalizó hace un mes.*

***Sr. Brown**: Erm...si, de hecho eso es por lo que estoy llamando…*

***Agente de Atención al Cliente**: Bueno, en realidad no me sorprende que llame usted ahora …Qué tal sus vaciones en Chipre? Estoy seguro de que su mujer y sus hijos disfrutaron del hotel de en el que se alojaron…*

***Sr. Brown**: Si, fueron unas vacaciones estupendas… y como es que usted sabe todo eso?*

***Agente de Atención al Cliente**: Pues porque obviamente esta en el sistema, Sr. Brown..... En cualquier caso, mejor empezar a buscar un nuevo trabajo... ya que dado el coste de sus vacaciones familiares y el pronto vencimiento del recibo del cocheo… por no mencionar el pago de la VISA realizado el 22 de este mes…*

***Sr. Brown**: Eso también está en su sistema?*

***Agente de Atención al Cliente**: si, por supuesto Sr. Brown. Por cierto, buena elección el libro que compró en Internet... Yo lo leí y me dió algunos buenos consejos …*

***Mr. Brown**: Hmmm...vale...en referencia al nuevo servicio de búsqueda de empleo, ¿necesito proporcionarles una foto mia actualizada?*

***Agente de Atención al Cliente**: No Sr. Brown, por supuesto que de eso ya nos hemos ocupado nosotros! Tenemos muchas fotografías recientes en nuestro sistema. Lo que me recuerda … bonito bronceado cogió en sus vacaciones! Debe haber tenido un tiempo magnífico! Antes de que me olvide, en relación a la foto, prefiere una con gafas o sin ellas?*

***Sr. Brown**: Oh...bueno....sin ellas está bien...Así que sobre mi registro,*

¿podemos fijar una cita para algún momento de la semana que viene?

***Agente de Atención al Cliente**: Permítame comprobar nuestro sistema… ¿Que tál el miercoles al mediodía? Oh, espere un segundo! Me acabo de dar cuenta de que usted tiene cita con el médico usto para ese momento. ¡Y estoy seguro de que no quiere perdersela, ya que seguramente es muy importante comporbar su nivel de colesterol ¿Qué tal el jueves a primera hora de la mañana, a las 9?*

***Sr. Brown**: El jueves por la mañana me viene bien… ¿Debo llevar conmigo documentos de algún tipo?*

***Agente de Atención al Cliente**: No Sr. Brown, ya tenemos toda la información que necesitamos en nuestro sistema.*

***Sr. Brown**: Estoy seguro que...*

***Agente de Atención al Cliente**: Gracias por llamar, Sr. Brown y nos vemos la semana que viene. Por cierto, disfrute de su cappuccino en el Cafe Ole'...*

***Sr. Brown**: Eso estoy haciendo...adios...*

...

Objetivos:
1. Primeras reacciones de los participantes incluyendo:

Posibilidad / imposibilidad del escenario

Aceptabilidad / inaceptabilidad del escenario

2. Creencias y actitudes de los participantes sobre cómo la tecnología afecta o podría afectar su privacidad

Después de presentar el escenario anterior al grupo, intente explorar en profundidad lo siguiente:

1a. ¿Cómo se sentirían si esto les pasara a ustedes?
(También intente establecer el grado de control / impotencia que sienten los participantes en este escenario hipotético)
1b. ¿Cómo reaccionarían ustedes si esto les pasara? ¿Qué harían ustedes?
1c. ¿Es un escenario <u>posible / imposible?</u>

1d. ¿Es un escenario <u>aceptable / inaceptable?</u>

2a. ¿Hasta qué punto creen ustedes que las tecnologías individuales "independientes" afectan a su privacidad?
2b. ¿En qué medida creen que las "tecnologías inteligentes", es decir aquellas que procesan datos de un modo automático (o semi-automático) afectan su privacidad?

3a. ¿Qué tipo de información personal piensan ustedes que

3. Creencias y actitudes de los participantes en cuanto al tipo de información, como: en el caso de informes médicos, datos financieros; fotos y ubicación.

4. Creencias y actitudes de los participantes sobre la recopilación, uso y distribución de información personal ante terceros.

5. Creencias y actitudes de los participantes sobre las ventajas e inconvenientes de ser vigilados

sería aceptable recoger, usar y / o compartir?

3b. ¿A qué tipo de información personal se opondrían ustedes a que fuera recopilada, usada y / o compartida?

4a. ¿Qué piensan ustedes acerca de que su información personal sea recopilada, utilizada y compartida por el estado?

4b. ¿Qué piensan ustedes acerca de que su información personal sea recopilada, utilizada y compartida por entidades privadas (como las comerciales)?

5a. ¿Creen que hay algún beneficio en el hecho de quesus acciones y comportamientos sean vigilados? 5b. ¿Creen que hay alguna desventaja en el hecho de que sus acciones y comportamientos sean vigilados?

Tiempo Total: 1 hour 15min

Reacciones a escenarios

[Unos 20 mins]

- *Estimular un debate con el fin de explorar las percepciones de los participantes sobre la dicotomía "seguridad versus privacidad"*

- *- Aquí, la discusión no debe centrarse en si estas tecnologías aumentarán la seguridad – Eso se debe tomar como un hecho. La discusión debe centrarse principalmente en si estas tecnologías afectan a la privacidad y por lo tanto giran en torno a la dicotomía"seguridad vs. Privacidad"*

Item 5

Durante el próximo ejercicio, vamos a discutir otra situación hipotética. Imaginen el siguiente escenario:

Debido a un incremento significativo de los crímenes violentos en la capital, incluyendo una serie de secuestros y asesinatos que parecen aleatorios y sin relación entre sí, el estado ha decidido introducir vigilancia CCTV en cada espacio público, tanto en lugares, de propiedad pública (como el metro, jardines e instalaciones públicas) como en aquellos otros de propiedad privada (como tiendas, centros comerciales, y taxis) que permitirán reconocimiento facial automático. Además, a todos los coches que pasen por los puntos principales de control se les grabará el número de la matrícula. También hay planes para instalar sensores en todas las áreas públicas, capaces de detectar sonidos altos como en caso de que alguien este gritando. A todos los ciudadanos se les exigirá la recogida de su AND y huellas dactilares y se les escaneará el iris. El Estado también ha decidido que todos los ciudadanos identificados como posible peligro para terceros, serán etiquetados electrónicamente para monitorizar y rastrear sus movimientos. Para su seguridad, las personas mayores y los niños de hasta 12 años serán también etiquetados electrónicamente. Toda la información proporcionada por las diferentes tecnologías será almacenada en bases de datos enlazadas, administradas por la policía, quien será automáticamente notificada si se produjese causa de alarma y peligro para algún ciudadano.

Diga a los participantes que vuelvan a imaginar el escenario anterior, pero con las siguientes variaciones:

Variación 1: A pesar de que se está produciendo un significativo incremento de los crímenes violentos en la mayoría de las ciudades vecinas, la ciudad en la que usted reside no está experimentando incremento alguno de crímenes. Sin embargo, el Estado decide introducir aún así medidas de vigilancia como precaución.

Variación 2: El país en su conjunto tiene en general un porcentaje de criminalidad muy bajo, pero aún así el Estado decide introducir medidas de vigilancia como precaución, después de que una ciudad vecina experimentara un incidente aislado en el cual algunas personas fueron disparadas y heridas gravemente por un hombre que abrió fuego en un centro comercial.

Durante el debate de la situación anterior y sus variaciones, intente explorar en detalle los siguientes factores y cómo podrían afectar a la dicotomía "seguridad vs privacidad ":

Objetivos:

1. Clima de seguridad y nivel de amenaza

1a. ¿Qué les hace sentirse seguros en el escenario propuesto?

1b. ¿Qué les hace sentirse vulnerables en el escenario propuesto?

1c. ¿Estarían ustedes dispuestos a sacrificar su privacidad si el nivel de amenaza fuera diferente, como en los casos de las variantes 1 y 2 del escenario?

2. Despliegue de tecnologías específicas

2. De las tecnologías inteligentes descritas en el escenario, es decir:

CCTV con reconocimeinto facial automático,
Reconocimiento Automático del número de matrícula (ANPR),
Sensores (con capacidad para detectar sonidos altos)
Tecnologías biométricas (incluyendo huellas dactilares)y
Etiquetado electrónico (que utiiza RFID)

2a. ¿Qué tecnologías consideran aceptables? ¿Por qué?

2b. ¿Qué tecnologías consideran invasivas y como una amenaza a su privacidad? ¿Por qué?

2c. ¿Qué piensa usted de estas tecnologías automatizadas (o semi-automáticas) mediante las cuales se toma la decisión final por parte del sistema y no por un operador humano?

3. Lugares de ubicación tales como: *Aeropuertos* *Centros Comerciales* *Calles*	***3a. ¿Qué lugares consideran aceptables para ser vigilados? ¿Por qué?*** ***3b. ¿Qué lugares consideran inaceptables para ser vigilados? ¿Por qué?***
4. Existencia de leyes y otras medidas preventivas (en relación con la recopilación, almacenamiento y uso de los datos)	***4a. ¿Qué piensan ustedes acerca de las leyes de privacidad? ¿Les hacen sentir protegidos?*** ***4b. ¿Existen algún tipo de garantías o condiciones que ustedes encontren tranquilizadoras?***
5. Duración del almacenamiento de los datos de vigilancia	***5a ¿Qué opinan de la duración temporal del almacenamiento de los datos de vigilancia? ¿Supone alguna diferencia?*** ***Para ayudarle en el debate, proporcione a los participantes los siguientes ejemplos:*** ***- Las grabaciones de CCTV*** ***- La ubicación y el movimiento de los coches*** ***- El almacenamiento de ADN, huellas dactilares e imágenes de iris*** ***- La localización de los ciudadanos que representan un riesgo para los demás*** ***- La localización y los movimientos de las personas mayores y los niños*** ***5b. Si el tiempo de almacenamiento contituye una diferencia, ¿qué consideran como un marco de tiempo aceptable?***
	Tiempo Total: 1 hour 35min

Objetivos	Sesión de resumen
Breve resumen del debate [5 mins]	***Item6*** ***Al final del grupo de referencia, es útil proporcionar un resumen de los puntos que hayan surgido en el debate. Aquí debe usted realizarun breve resumen de los temas y cuestiones planteadas durante el debate. Después, puede usted preguntar lo siguiente a los participantes:***

▪ *Confirme los principales acuerdos alcanzados* ▪ *Proporcione una oportunidad más para profundizar en lo que se haya dicho*	- **¿He resumido bien lo que se dijo hoy aquí?"** - **"¿Hay algo que nos hayamos olvidado?"** - **"¿Hemos cubierto todos los temas?"** ***Esta breve sesión dará a los participantes una oportunidad adicional para expresar sus puntos de vista y también se puede utilizar para ampliar más los temas que se hayan planteado, pero no cerrado en su momento.*** ***Tiempo Total: 1 hour 40 min***

Objetivos	Clausura
Conclusión del grupo de referencia **[5 mins]** ▪ ***Agradezca a los participantes*** ▪ ***Entregue el reembolso*** ▪ ***De información sobre SMART***	***Item 7*** **Con este último ejercicio nuestro debate ha llegado a su fin. Permítanme aprovechar esta oportunidad una vez más para agradecerles el haber estado con nosotros y por compartir sus opiniones, experiencias y reflexiones.** ***En este punto, entregar los reembolsos a los participantes e informarles sobre los pasos siguientes.*** ***Darl a los particpantes que lo soliciten más información sobre SMART*** ***Total: 1 hour 45 min***

APPENDIX D – DEBRIEFING FORM

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

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

APPENDIX E – CONSENT FORM

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

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

1.1. Commercial space

1.1.1. Awareness of different surveillance methods/technologies

1.1.1.1. CCTV

1.1.1.2. Loyalty cards

1.1.1.3. Security guards and store detectives

1.1.1.4. Security tags on merchandise and electronic gates

1.1.2. Perceived purposes

1.1.2.1. Theft prevention

1.1.2.2. Security purposes

1.1.2.3. Commercial objectives

1.1.2.3.1. Collection of customer data

1.1.2.3.2. Marketing

1.1.2.3.3. Financial data

1.2. Boundary space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. Personal data checks

1.2.1.1.1. Examination of passports

1.2.1.1.2. Identity cards

1.2.1.1.3. Visa

1.2.1.1.4. Criminal records

1.2.1.1.5. Bank data

1.2.1.2. CCTV with AFR

1.2.1.3. Luggage checks

1.2.1.4. Metal detectors

1.2.1.5. Security agents and law enforcement personnel and sniffer dogs

1.2.2. Perceived purposes

1.2.2.1. National security

1.2.2.2. Passenger safety

1.2.2.3. Prevention of crime

1.2.2.4. Commercial reasons

1.2.2.4.1. Marketing

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV

1.3.1.2. Purchase of tickets

1.3.1.3. Turnstiles

1.3.1.4. Frisking of visitors

1.3.1.5. Scanning of bags

1.3.2. Perceived purposes
1.3.2.1. Security
1.3.2.2. Crime investigation
1.3.2.3. Collection of personal data
1.3.2.4. Organisational reasons
1.3.2.5. Restrict visitors to enter with alcohol and firecrackers
1.3.2.6. Prevention of vandalism and theft
1.4. Mobile devices and virtual spaces
1.4.1. Awareness of different surveillance methods/technologies
1.4.1.1. Phone tapping
1.4.1.2. Location tracking via GPS
1.4.2. Perceived purposes
1.4.2.1. Crime-related purposes
1.4.2.2. Commercial and marketing purposes
1.4.2.2.1. Collection of data
1.4.2.2.2. Selling of customer data
1.4.2.2.3. Improve technical capacities of mobile devices

2. Perceptions and attitudes towards smart surveillance and integrated dataveillance
2.1. Feelings
2.1.1. Extreme discomfort
2.1.2. Fear
2.1.3. Helplessness and anger
2.2. Behavioural intentions
2.2.1. Active reactions
2.2.1.1.1. Counteract
2.2.1.1.2. Take legal action
2.2.1.1.2.1. Report illegal behaviour
2.2.1.1.2.2. Contact a lawyer
2.2.1.1.3. Engage in self-protection strategies
2.2.1.1.3.1. Share less data
2.3. Beliefs
2.3.1. Likelihood of massively integrated dataveillance
2.3.1.1. Technical aspect
2.3.1.1.1. Rapid development of technologies
2.3.1.2. Ethical aspect
2.3.1.2.1. Private and public organisations
2.3.1.3. Legal aspect
2.3.1.3.1. Restrictions of laws
2.3.1.3.2. Changing conditions
2.3.2. Acceptance of massively integrated dataveillance

2.3.2.1. Invasion of privacy
2.3.2.2. Notion of control
2.3.2.3. Power imbalance between state and citizens
2.3.2.4. Accessibility of data between public authorities
2.3.2.4.1. Threat to privacy and freedom
2.3.2.5. Perceived purpose and necessity of data collection
2.3.2.5.1. Crime prevention and investigation
2.3.2.6. Type of data
2.3.2.6.1. Basic data
2.3.2.6.2. Sensitive data
2.3.3. Perceived effectiveness of smart technologies and dataveillance
2.3.3.1. Decision-making capabilities of automated systems
2.3.3.1.1. Less intrusion
2.3.3.1.2. Subjective decision taking by humans as risk
2.3.3.1.3. Less manipulation
2.3.3.1.4. Reliability
2.3.3.1.5. Final decision and reasoning by a human
2.3.3.2. Circumvention of technologies by criminals

3. Security-privacy trade-offs

3.1. Acceptance of technological surveillance
3.1.1. Feelings
3.1.1.1. Intrusion of privacy
3.1.1.2. Vulnerability and insecurity
3.1.1.3. Indignation
3.1.1.4. Helplessness
3.1.2. General beliefs
3.1.2.1. Violation of rights
3.1.2.2. No deterrent effect
3.1.2.3. General criminalisation of citizens
3.1.2.4. Lack of trust into citizens
3.1.2.5. Unjustified surveillance of citizens
3.1.2.6. Unclear motivations of surveillance
3.1.2.7. Misuse of citizens' data
3.1.2.8. Risk of corruption
3.1.2.9. Higher acceptance for high risk areas
3.2. Perceptions of different technologies
3.2.1. CCTV
3.2.1.1. Process of normalisation
3.2.1.2. Increase in feelings of personal safety
3.2.2. AFR

3.2.2.1. Violation of privacy
3.2.3. ANPR
3.2.3.1. Effectiveness
3.2.4. Sound sensors
3.2.4.1. Efficiency for crime intervention
3.2.4.2. Wrong conclusions
3.2.5. Biometric data
3.2.5.1. Vulnerability
3.2.5.2. Risk of DNA theft
3.2.5.3. Link to health data
3.2.5.4. Efficient for the investigation of crime
3.2.6. Electronic tagging (RFID)
3.2.6.1. Useful for criminals
3.2.6.2. Useful for specific societal groups
3.2.6.3. Voluntary basis
3.2.6.4. Invasion of privacy
3.2.6.5. Control of citizens

4. Surveillance laws and regulations

4.1. Trust in the state and effectiveness of legislation
4.1.1. Dissatisfaction with the protection by the state
4.1.2. Privacy breaches
4.1.3. Insufficient enforcement
4.1.4. Trust in Data Protection Agency
4.2. Length of data storage and accessibility
4.2.1.1. Purpose of data collection
4.2.1.2. Acceptance for security reasons
4.2.1.3. Access only by law enforcement agencies
4.2.1.4. Risk of manipulation
4.2.1.5. Threat of misuse
4.2.1.6. Unknown development of politics
4.2.2. Data sharing between different actors
4.2.2.1. Sharing with public authorities
4.2.2.1.1. Power imbalance between citizens and state
4.2.2.2. Sharing with private actors
4.2.2.3. Lack of citizen questioning data sharing