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

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

April 2014

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

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

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

Table of Contents

1. Key Findings

This document presents the results for France 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 dataveillance, the massive integration of data from different sources, and the "security versus privacy trade-off".

The French participants were in general highly aware of being under surveillance in different contexts including commercial, boundary and public spaces. When discussing these contexts, a wide range of surveillance technologies and methods was mentioned including video-surveillance, loyalty cards, biometric surveillance and the use of different object and product detection devices. Participants were also aware of possible monitoring via the use of mobile devices and in this regard mentioned GPS location tracking and the recording of conversations. Overall, participants perceived surveillance in these contexts as taking place primarily for security-related purposes, including the prevention and investigation of crime. Additionally, with regards to the collection of data by private companies, most participants were aware of commercial motivations including those related to marketing and advertisement purposes.

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. The possibility of massively integrated dataveillance was discussed from a technical viewpoint, and, to a lesser extent from legal and ethical perspectives. Dataveillance was perceived as technically possible, although not to the extent as depicted in the scenario, though some participants mentioned that this would be both illegal and unacceptable. Participants also questioned their own role in the sharing of personal data and in particular perceived online data sharing by citizens as significantly increasing the possibility of occurrence of massively integrated dataveillance. Moreover, with regards to participants' acceptance of integrated dataveillance, it appears that this was contingent on a number of factors including type of data collected, purposes of use, and whether consent for data sharing was provided. Participants also took into consideration any possible benefits for citizens and risks of data misuse. In general it appears that dataveillance was perceived as more acceptable when it provided a certain benefit to citizens, such as an increase in security or a more efficient service for customers. All in all, it seems that participants preferred their data to be used by the state for administrative and crime-related purposes, rather than for commercial reasons by private actors.

During the discussion of the “security-privacy trade off” scenario, it appears that the extensive use of surveillance made participants feel extremely uncomfortable and vulnerable for a number of reasons. Firstly, participants appeared concerned that the use of intrusive surveillance would not only impinge on the privacy and freedom of citizens but also possibly result in a process of dehumanisation. Additionally, concerns about the possible misuse of technologies and surveillance data by the state were also raised. Moreover, most participants challenged the notion that an increase in surveillance would provide more security, since they perceived surveillance as inefficient in relation to crime prevention, one of the reasons being that surveillance can be circumvented. In spite of these predominant viewpoints, a minority of participants did believe that, to a certain extent, surveillance technologies had a deterrent effect. With regards to the investigation of crime, the findings indicate that most participants regard surveillance as useful.

Participants were also asked about their views on the different types of surveillance technologies mentioned in the scenario. Different technologies seemed to meet different levels of acceptance: while CCTV was widely accepted in public spaces, most participants objected to the use of biometric technologies, especially those involving the use of DNA. Similarly, the use of electronic tagging was considered as totally unacceptable since it was perceived as a threat not only to privacy but also to citizens’ freedom. Nevertheless, the use of this surveillance tool was considered as acceptable in case it was employed for the monitoring of ex-convicts.

Finally, participants were also invited to share their viewpoints regarding the extent to which they trust the state with citizen data. The participants were also asked to suggest an appropriate length of storage for surveillance data. In general it appears that the majority of participants trusted the authorities with the collection and use of citizen data, with several participants arguing that unless there is a valid and justified cause, citizens are not the focus of extensive surveillance. Therefore it appears that most participants were generally not concerned that the state could misuse surveillance data. In relation to length of data storage, opinions were rather mixed; while a number of participants appeared to prefer specific limitations of storage times in order to avoid potential misuse of data, others claimed that longer storage times are necessary in order to allow access to surveillance data should the need arise, such as in cases of crime investigation.

2. Introduction

The analysis 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 The International Criminal Police Organisation (INTERPOL) was responsible for the translation and back-translation of the research materials and Morpho (MPH) took care of the commissioning of the focus groups. The moderation of the focus groups and transcription of discussions were carried out by A2S Communication in Paris.

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

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

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

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

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research project. The focus groups in France were carried out on the 19th, 20th, and 21th November 2013 in Paris[2]. The composition of the groups held in France 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.

[2] It should be noted that the three focus groups were conducted subsequent to the Boston Marathon bombings and the disclosures by Edward Snowden with regards to the mass surveillance programs undertaken by the National Security agency (NSA). However, it does not appear that these occurrences influenced the participants' views on government surveillance.

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 French version of the discussion guidelines can be found in Appendix C.

3.3 Focus group procedure

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

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

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

3.4 Data analysis

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

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	F	F
P2	M	F	F
P3	M	M	F
P4	F	M	M
P5	F	F	M
P6	M	M	F
P7	F	M	M
P8	F	M	M
P9	M	F	F
P10	No-show	No-show	M
Total	**9**	**9**	**10**

The atmosphere in all focus groups was described as friendly, free-flowing and cooperative, and the moderators had the impression that most participants felt at ease in sharing their opinions. However, slight differences in the group dynamics between the three groups were observed by the moderators.

In Group 1 (18-24 years), participants were generally described as being enthusiastic and cooperative. Most of the participants appeared keen to participate in the discussion and according to the moderators some had firmly established opinions on the topic. A number of participants stood out for different reasons; while one of the participants (P3) was described as *"disruptive"* by the moderators and often tried to dominate the discussion, two other participants were considered as less assertive than the rest of the group. On a general note, the participants in this group were said to have displayed the highest interest in the project and requested more information about the research after the end of the discussion.

The atmosphere in Group 2 (25-44 years) was described as friendly and cooperative. It seemed that participants enjoyed discussing their different viewpoints and appeared well engaged with the topic. In addition, the flow of the group discussion was perceived as mainly consistent throughout the whole session, except for the contributions of one of the participants (P7) who appeared rather enthusiastic about expressing his views and thus at times attempted to dominate the discussion. On the other hand, one of the participants (P1) was described as having a more reserved attitude. In general the moderators pointed out that on a number of occasions, the discussion had to be refocused on the topic since participants tended to deviate from the main theme.

Participants of the third and final focus group (45+ years) were described as eager to share their ideas and opinions and displayed a thorough knowledge of the use of surveillance in their daily lives. The

group was regarded as an extremely dynamic one and the discussion was considered as free-flowing and as generally constructive. The moderators pointed out that two participants appeared more reserved than others, but still contributed in a constructive manner from time to time.

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 commercial spaces, specifically in the context of a supermarket, all focus group participants displayed a high awareness of being surveilled. Video-surveillance systems and the use of loyalty cards were perceived as the predominant methods through which consumers are monitored in this space. Perceived purposes of surveillance differed according to type of monitoring method; while most participants perceived CCTV to be used for security-related purposes, the use of loyalty cards was regarded as fulfilling commercial functions. In addition, one participant also briefly mentioned surveillance by security guards.

The use of surveillance cameras was perceived as ubiquitous by the majority of participants: "*There are always cameras in supermarkets watching our every move and where we go*" (P7-I). While several participants believed that CCTV systems were used for the prevention of crime by observing suspicious customer behaviour, other participants believed that CCTV was not used for prevention purposes but rather for the investigation of crimes. In fact the latter participants believed that the recordings were not watched in real time, but only after an incident had occurred.

Loyalty cards in supermarkets are believed by participants to be utilised by commercial entities in order to collect customers' personal data and to monitor buying behaviour. A number of participants perceived that data such as name, date of birth, home and email address was "*systematically requested*" (P9-II) when they applied for a loyalty card. While the collection of such basic information appeared to be tolerated by the majority of participants, other personal data, such as information about salary or children, was perceived as irrelevant and inappropriate: "*How many children I may have and things like that, I do not think that should have anything to do with a loyalty programme*" (P1-I). In addition, a number of participants were aware that such data was passed on to various third parties for advertising purposes: "*I think they share the information with other people, because I get phone calls and emails from people I do not know*" (P9-III). However some participants regarded the sharing of personal data with third parties as acceptable once the customer's permission for data sharing is obtained: "*We are asked if the information can be passed on to other parties*" (P5-II).

In addition to the collection of personal data for advertising purposes, participants also mentioned the use of loyalty cards as a tool to monitor customers' buying behaviour. Participants believed that purchasing habits were monitored and utilised for market research in order to enhance the shops' shelf and product organisation. Additionally, several participants also mentioned that customer data was utilised with the aim of increasing sales and turnover. Many participants expressed their discomfort at being monitored and not knowing what their data would be used for: "*We do not see what goes on behind the scenes, [...] I feel like I am the subject of some sort of study*" (P1-I). Although the majority of participants pointed out that in their opinion, market research based on their personal data was "*mainly about profitability*" (P7-III), on the other hand other participants regarded this as a positive aspect, because from their point of view it could "*improve the quality of services*" (P10-III) for customers.

5.1.2 Boundary Space

In the context of border control, the discussion mainly focused on an airport setting as a boundary space. At the outset, the awareness of pervasiveness of surveillance in airports by various surveillance measures was evident in all focus groups: "*It is the place you are observed the most*" (P1-I). Participants pointed out that the surveillance of travellers' data is already underway before travellers physically enter the airport: "*The information is always passed on when we buy a ticket. It is compulsory for the travel agent and administrative authorities. When we apply for a passport personal information is shared*" (P4-II).

A variety of surveillance measures was mentioned by the participants in this context, including the monitoring of personal data through passport and identity checks, the use of biometric technologies for identification purposes and possible interrogations by customs personnel. Participants also mentioned the use of a number of object and product detection devices, including luggage controls, and screening by full body scanners, in order to prevent the trafficking of illegal and counterfeit goods. In addition, traveller habits were also perceived as being monitored by airline companies via customer loyalty programs such as the frequent flyer program. In relation to data sharing between entities, it appears that participants believed their data to be shared among the various parties involved in an airport context, such as national security services, including law enforcement agencies and customs agencies, as well as with airport personnel and private security companies.

Participants perceived national security and passenger safety as the predominant purposes of surveillance at airports. It seems that the intensification of surveillance measures in this context was ascribed mainly to fears in relation to terrorism: "*Everyone is worried about terrorism since September 11*" (P7-I). Most participants appeared to be highly aware of the rigorous monitoring measures undertaken for the prevention of crime at border controls for purposes of national security: "*It is an illusion to think people are not being monitored when they travel back and forth between different places. It is all designed to make sure that undesirable people do not enter the country*" (P7-II).

Moreover, participants also believed that travellers with *"risky profiles"* (P7-III) were scrutinised more closely than others by airport personnel: "*Customs officers have profiles of people they will always check, they have specific data regarding individuals to stop, the way they dress and their nationality for example*" (P8-II). Although these measures were regarded as justified for security-related purposes, participants expressed their discomfort at being interrogated by customs and immigration officers about their reasons for travelling. In this regard, some participants expressed their belief that travellers were given no choice regarding the disclosure of information: "*I was coming back from Morocco and they asked me where I was going and what I was going to do there. I had no other choice but to explain; otherwise they would have arrested me*" (P8-II).

Additionally, some participants perceived a number of differences between surveillance measures at airports in Europe and those outside of Europe: in comparison to the measures used at European airports, certain measures at other airports were considered as "*extraordinarily intrusive*" (P3-III). Participants specifically alluded to the use of full body scanners at non-European airports, which they perceived as a great threat to privacy: "*There are some scanning machines that really do undress you, they go much further and examine your whole body*" (P4-III).

On a last note, although it appeared that most participants regarded general safety measures at airports as necessary for the prevention of crime, some participants perceived the increase in security measures for the fight against terrorism to be used as a pretext for surveillance which is more extensive and intrusive in nature: "*They have a cast-iron excuse to do it, they can do whatever they like*" (P3-I).

5.1.3 Common Public Spaces

In common public places, specifically at large public events such as sports games and concerts, and also in public institutions such as museums, participants expressed their awareness of several surveillance measures, including CCTV systems and object and product detection devices. Participants also made reference to the collection of personal data by the event organisers once tickets are purchased. The presence of security guards on the premises or during the event was also mentioned. In general, these measures in common public spaces were seen by the majority of participants to be used for security purposes: "*It is for our security*" (P5-III).

The findings indicate that the use of CCTV systems, which was perceived as a primary means of surveillance in all focus groups, appears to have gone through a process of normalisation in the public sphere: "*It is almost the norm now to be filmed*" (P4-II). Apart from surveillance cameras, some participants also drew attention to the possibility of being inadvertently recorded at large events by television cameras filming the event. In general, surveillance measures were perceived as enhancing security both for the audience as well as for the event performers or players: "*[It is for] safety, given that at major events, there are large crowds and it is important to ensure the safety of the players and the people who go to watch them*" (P9-II). However, some participants argued that these safety measures were insufficient to counteract certain unforeseeable events such as in cases of mass panic: "*If something is going to happen, it will happen, a stampede at a concert happens very quickly*" (P7-I).

The use of surveillance in other public spaces such as museums was also discussed; once again, in this context the use of CCTV systems for the protection of property and artefacts was mentioned. Participants also mentioned checks by security guards who either manually examined visitors' hand bags or else used product detection devices in order to check for prohibited objects. Some of the participants criticised these safety measures on the basis that they were solely taken with the aim of protecting the artefacts on display rather than increasing the security of the visitors: "*Unfortunately a work of art is worth more than a human being*" (P3-I).

5.1.4 Mobile Devices and Virtual Spaces

Participants mentioned a variety of ways in which surveillance occurs through the use of mobile telecommunication devices, including the recording of conversations, GPS location tracking and the collection of data through the use of mobile internet and smart phone applications. In general, the recording of conversations was perceived to be conducted for crime-related purposes, whereas GPS location tracking and the collection of personal data about consumption habits were considered to have a commercial function.

Participants perceived the recording of conversations as certainly possible by state and intelligence agencies: "*[…] if the state wants to, it can record what you say*" (P7-I). Nevertheless, the majority of participants argued that this type of surveillance was not conducted on "*ordinary citizens*" (P9-III) but rather on those suspected of crimes: "*The intelligence agencies, we are watched all the time, they have the means to record us, but they only do if they have good reasons to*" (P9-I). In spite of this, however, participants also believed that people could be monitored after having accidently drawn attention to themselves by using specific "*key words*" (P2-I) which were classified as risky by the government. Furthermore, participants also expected mobile operators to generally be obliged to keep mobile phone data logs for years in case such information was required by government agencies for crime-related purposes.

In the context of GPS location tracking, the participants were of the belief that location data could be shared with third parties for commercial reasons: "*All operators know where our telephones are at any time and can pass on the information*" (P8-II). Moreover, location data was considered as accessible to other private companies through the use of smart phone applications. It appears that this monitoring was regarded as akin to "*spying*" (P3-III) on customers and thus as posing a serious threat to privacy: "*It is an open door to our private lives*" (P3-III). Most of the data which was collected by companies through mobile phone applications was believed to be used for market research purposes, especially with regards to new product development: "*So that they can understand the way we live, think and react... They get inside our heads to develop the products of the future*" (P3-II).

Participants also expected mobile phone manufacturers to have access to customers' data and to collect it. In this regard, participants appeared concerned that these companies could have access to biometric

data such as in cases where customers use a fingerprint scanner to unlock their mobile phones: "*The system can recognise a finger print, so you imagine that the system can send this information to Apple*" (P7-II). In addition, many participants were concerned about possible accessibility to personal documents when saving data from their phone on the cloud: "*What frightens me with mobile phones is all the photos you take, you can store them on a virtual hard drive and I wonder who can access them!"* (P9-I).

5.2 Perceptions & Attitudes towards Smart Surveillance and Integrated Dataveillance

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

5.2.1 Feelings

After having listened to this conversation, the focus group participants revealed a wide range of feelings including disbelief, extreme discomfort, fear, helplessness and indignation. In general it appears that such feelings resulted from the participants' perception that the scenario involved a violation of boundaries. A few participants expressed a positive feeling, mainly due to the consideration that such a situation could, to a certain extent, be convenient.

In general, strong negative reactions to the scenario were expressed throughout all focus groups. Firstly, some participants showed disbelief and surprise at the portrayed situation; comparing the scenario to *"a bad horror movie*" (P1-I), they argued that the scenario *"is a bit far-fetched"* (P1-I). In general, participants appeared anxious that such extensive surveillance could indeed become reality and perceived the situation as *"scary*" (P1-II).

Overall, most participants perceived the situation as *"intrusive"* (P4-III) and as amounting to *"spying"* (P9-III) on citizens; as a result, several participants felt "*outraged*" (P7-I) at the mere idea of such extensive surveillance: "*I [would] feel [like] I am living in a glass house, [where] people know what I eat, when I sleep*" (P3-II). As a consequence, it appears that the majority of participants perceived a violation of boundaries at the disclosure of such personal data: "*Nothing is private anymore*" (P3-III). In addition to privacy issues, participants also voiced their concerns on the effect this would have on citizens' freedom: "*There will be no freedom anymore*" (P8-I). In fact, this appeared to lead to feelings of helplessness among participants "*I would feel trapped*" (P4-I).

On a last note, a minority of participants expressed positive feelings with regards to the scenario. In this case they primarily regarded such monitoring as providing convenience to the service user: "*The only practical thing is that she has all the information and I will not have to fill in all the job centre forms*" (P5-I).

---

[3] Clarke, R. (1997)

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

5.2.2 Behavioural Intentions

In addition to asking about their feelings, participants were also asked for their resulting behavioural intentions. In general, it appears that those participants who felt a strong sense of discomfort and a violation of boundaries revealed the need to take personal action in order to avoid, or at least to limit, the sharing of their data: "*You have to defend your own privacy"* (P7-II). Participants claimed they would change their behaviour by for instance minimising the amount of data they shared on a daily basis: "*I myself can control the information, let's say, I can vary the extent to which I divulge information*" (P3-II). Other participants, perceiving this situation as illegal, declared that they would take legal action in order to protect their privacy: "*I would consult a lawyer; you have no right to share information*" (P3-III).

As opposed to the majority of participants, a minority displayed less resistance to being surveilled; perceiving themselves as law-abiding citizens, they appeared to express indifference at being monitored: "*In any case, I could not care less about cameras, I have nothing to hide*" (P2-II). Moreover, as mentioned above, a minority of participants perceived the use of surveillance and massively integrated dataveillance as facilitating bureaucratic procedures; consequently they appeared willing to be monitored in exchange for a certain level of convenience: "*I am happy to give out information if it makes my daily life easier*" (P3-II). Lastly, other participants pointed out that such monitoring was part and of 'modern society' and thus rather unavoidable: "*If we want to move with the times, we have got no choice*" (P7-I)

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), participants predominantly discussed this mainly from a technical aspect, although some participants additionally mentioned legal restrictions and ethical concerns. Participants also discussed general aspects of data sharing and in particular questioned their own role in the sharing of personal data.

Overall, although the scenario was perceived as *"not very realistic"* (P2-III), the majority of participants regarded the hypothetical situation as *"credible"* (P7-I), though not to the extent portrayed in the scenario. From a technical perspective, several participants argued that such a situation would be possible given that the data, though currently split-up in different parts, is indeed available: "*It is a risk because the information exists*" (P8-III). Nevertheless, perceiving such a practice as illegal, a minority of participants argued that current legislation would present an obstacle to extensive surveillance and to unrestricted integrated dataveillance: *"It's not possible […] You cannot just do anything you like, there are laws against it*" (P9-III). Moreover, others underscored the ethical aspect and argued that it is *"not acceptable"* (P3-III) since it would affect not only citizens' privacy but most fundamentally also their freedom. However, in spite of such reservations, it seems that a number of participants believed that such a development would be likely in the near future: "*we are well on track*" (P4-II) and argued that

such practices might eventually undergo a process of normalisation: *"[…] and maybe we'll accept it […] we accept things our parents would never have accepted"* (P7-II).

Participants also appeared to make sense of the scenario by linking it to the use of social media and in relation to this, most participants seemed well aware of the possible risks of data sharing in virtual spaces. Several participants pointed out that people contributed voluntarily to the spreading of their personal data, even if this was often done unintentionally: "*People talk about privacy but don't we already give up a lot of information about ourselves?*" (P2-II). Consequently, some participants argued that more awareness is needed with regards to the consequences of online data sharing: "*People still need to be educated a bit more about social media […] all these technologies, lots of people adopt them without realising the impact they can have*" (P6-II). These participants perceived data sharing on social networks not only as significantly increasing the possibility of occurrence of massively integrated dataveillance, but also as increasing the risks of data misappropriation and misuse: *"We are already half way there, when we are ready to divulge our private lives via social media and people with good or bad intentions can use this information [...] It's easy to trace loads of information about us"* (P4-II).

Lastly, notwithstanding the role and responsibility of the individual citizen in data sharing, some participants argued that divulging personal data is, at times, unavoidable. In this regard, participants expressed difficulty and frustration at how they can potentially limit the disclosure of personal data in certain situations: "*But sometimes we do not have any choice, we are asked for information all the time, we do not realise it, we fill in stuff, we give loads of information*" (P1-I).

5.2.3.2 Acceptance of massively integrated dataveillance

Overall, it appears that the opinions of most participants were rather mixed and that acceptance of massively integrated dataveillance depended on several criteria, including type of data, whether consent for data sharing is expressly given and purposes of data collection, use and sharing. In addition, it appears that perceived risks of data misuse also had a bearing on acceptance of dataveillance.

Primarily, it appears that the main criterion for the acceptance of dataveillance was the type of data collected. The majority of participants agreed upon the acceptability of sharing a minimum amount of personal data, including name, age, marital status and number of children, photos and professional information. On the other hand, participants objected to the sharing of more confidential data, such as financial information and medical data, especially in cases where such data sharing was perceived as irrelevant and unnecessary. Nevertheless, some participants pointed out that when such sharing is carried out in an appropriate and contained manner, such as the sharing of health data between health professionals, this could provide certain benefits:

> *"If your files can be accessed by doctors and specialists, if it stays within the medical context, and the pharmacist too is able to see your prescriptions if you run out of medication when you are away from home [...] So you can go anywhere in France and the pharmacist can help you out, this is a good thing" (P3-III).*

Furthermore, some participants expressed their wish of their data being shared solely if they consented to it: "*Not if I do not know about it, if I have not agreed to make it public*" (P7-II). In addition to consent, another important aspect influencing acceptance of dataveillance was the purpose of data collection. Firstly, participants distinguished between the collection and use of data by private or public entities. Overall it appears that participants perceived both advantages and disadvantages in the manner that their data is used by different entities. The collection and use of data by the state for administrative purposes and for security-related reasons such as the prevention of crime appeared to be accepted: "*We ordinary citizens have nothing to hide and [...] it is reassuring to know that the state also collects information about people who are a potential danger to society*" (P2-II). With regards to private entities, participants perceived *"the commercial aspect"* (P2-I) as a major driver and in this respect, participants appeared concerned at the increase in the possibility of misuse. In particular, some participants appeared alarmed at the possibility that security gaps could be exploited by hackers: "*There are hackers who spend their time trying to hack into competitors' databases*" (P2-I).

On the other hand, a minority of participants perceived dataveillance as useful in cases in which the collection of data was considered as facilitating customer convenience, such as in the case of commercial establishments using a loyalty programme, which would allow to provide a better service to the customer based on peoples' shopping preferences: "*There is the privileged aspect of things, you arrive, you have the card, people know what you want*" (P1-I).

5.2.3.3 Perceived effectiveness of smart technologies

When discussing the effectiveness of surveillance technologies, participants differentiated between traditional surveillance 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. In general, participants appeared sceptical with regards to the automated decision-making process of smart technologies since they perceived such a process as too rigid when compared to the human decision-making process: "*For the time being we have not yet come up with a machine capable of thinking like a human being*" (P7-II). Similarly, while arguing that the use of technology in the surveillance process is cost-effective, it appears that participants' mistrust prevailed towards machines acting as a substitute to humans: "*There may be [financial] savings but we are forgetting the human input. [...] Can it replace people?"* (P2-I). Therefore, it appears that the human element in the surveillance process was considered as necessary by these participants.

5.3 Security – Privacy Trade-Offs

5.3.1 Acceptance of Technological Surveillance

In order to gauge the 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 participants. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging of vulnerable groups. The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[5].

When discussing the scenario, participants generally revealed an intense reaction: *"This shocks me greatly"* (P3-III). Perceiving the extensive use of surveillance technologies by the state as an invasion of privacy, they considered intensive surveillance as unacceptable: "*Peoples' private lives have to be respected by the state*" (P1-I). It appears that smart surveillance technologies raised feelings of vulnerability and insecurity among the participants in all the groups, who believed that the use of these tools would violate citizens' rights by "*labelling*" (P2-I) individuals; in this regard several participants expressed feelings of indignation at what they perceived to be a process of dehumanisation: "*The state is treating us like cattle!"* (P7-II). Moreover, participants conveyed concern at the possibility of data misuse by the state, which appeared to result in feelings of helplessness for some; here the participants alluded to historical events, such as the Holocaust, during which data about personal characteristics was misused for discrimination purposes: "*It all depends on how it is used, we should not forget the past [...] who knows*" (P9-III). Additionally, some participants expressed concern in relation to what could possibly happen to the stored surveillance data in case of a possible change in government: "*In 10 years' time with another government we do not know what they might do with it all […] frankly I am slightly uncomfortable with it*" (P3-III).

Alongside participants' fear of personal data being misused, many participants scrutinised the motivations of the state behind the deployment of surveillance technologies and questioned whether surveillance would be used solely for security-related purposes: "*I question it all, [what is] behind the security argument, they monitor us, I wonder why they spend so much money, if where I live there are no problems, I wonder why*" (P9-I). While participants objected to the indiscriminate monitoring of all citizens, a number of participants appeared in favour of the selective monitoring of criminals and suspects; in this regard, these participants claimed that such surveillance would make them feel considerably safer: "*Monitoring potentially dangerous people [would make me feel safe] [...] anybody would be reassured to know that such and such a person is being monitored*" (P1-I).

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

When participants were confronted with a significantly increasing crime rate in the second variation of the scenario, most participants did not noticeably change their opinions, since they considered privacy to be more important than security and perceived the indiscriminate surveillance of all citizens as posing serious limitations to citizens' freedom. This point of view appeared to be consolidated by participants' doubts that an increase in surveillance would result in more security. Such doubts were due to a number of reasons; firstly, participants were of the opinion that while the intentions of petty criminals could possibly be altered by the presence of surveillance technologies, this was not the case for more dangerous criminals: "*It will dissuade people from committing minor offenses, but not people with sick intentions"* (P3-III). Secondly, others pointed out that these measures would simply be circumvented in one way or another. In spite of these reservations, however, a minority of participants appeared to believe that surveillance does contribute, to a certain extent, to a lower crime rate.

Although beliefs in relation to the effectiveness of surveillance for crime prevention were somewhat mixed, surveillance was expected to be generally useful for the investigation of crimes: "*It will make it easier to investigate but it will not stop anything"* (P1-III). With regards to crime investigation purposes, some participants appeared willing to be monitored if it was proven that surveillance was effective for such purposes: "*If it helps to solve crimes, I am all for it*" (P3-II). Besides, a number of participants also mentioned as an advantage the possibility that surveillance data could be used in order to prove people's innocence: "*It can be used to exonerate people too; it can prove you were at a certain location*" (P2-II).

Lastly, in line with the above mentioned doubts that surveillance would contribute to the prevention of crime and thus to an increase in security, a number of participants believed that it was more important to search for the roots of criminality: "*The causes [for crimes] are the main issue; they have to be identified above all, rather than sanctioned. An entire system is put in place to target errors rather than to correct them*" (P7-II).

5.3.2 Perceptions of Different Technologies

In general, different types of surveillance technologies seemed to meet different levels of acceptance. While the use of CCTV and sound sensors was on the whole considered as acceptable by the majority of participants in public places, the other technologies depicted in the scenario were generally deemed as unacceptable. Biometric technologies and electronic tagging were, with few exceptions, perceived as being too intrusive. Primarily it appears that participants were concerned that the state, by using security as a pretext for the introduction of these surveillance measures, could possibly misuse such technology to its advantage in order to control citizens: "*We are speaking about a way for the state to keep tabs on the population as a whole... [...] it is what every state dreams of*" (P7-II).

In relation to video-surveillance systems, the use of CCTV appeared to have undergone a process of normalisation. This was in particular reflected by a number of focus group 3 (45+ years) participants who did not show any concern in relation to being filmed and who did not perceive any negative effect on

their privacy: "*I am not sacrificing my privacy, cameras do not bother me*" (P7-III). In particular, the use of video surveillance in public spaces appeared to be widely valued for enhancing feelings of personal safety. In this regard, cameras with face recognition tools were especially regarded as contributing to the identification of registered criminals, and some participants considered this function as resulting in a higher level of safety for citizens:

> "*I think a camera to pick out faces is a good thing for people considered to be dangerous, the security services or rather the computers will make the connection [...] and there will be greater surveillance, it means more security for me" (P4-III).*

In fact it appears that smart CCTV was regarded as more effective for the prevention of crime when compared to traditional video-surveillance systems: "*Above all we have to remember that most of the time no one is looking at these cameras, there are lots of images but few people look at them, and so it is only when they have to, that images are analysed, [which is] a painstaking task" (P7-III).* Nevertheless, albeit smart CCTV was considered as more effective, some participants also alluded to the risk that such devices could be misused by the authorities in order to spy on individuals, which appeared to worry a number of participants.

With regards to sound sensors for the recognition of screams and noises, most participants perceived such devices as acceptable, mainly due to the belief that they could prove efficient in providing more security to those considered as more vulnerable: "*It could be useful for women after a certain time of the day*" (P3-III). Nevertheless, some participants regarded sound sensors as being rather inefficient for crime prevention and intervention, since they argued that the crime would have been already committed when the police arrived on scene: "[...] *it is pointless, they will pick up a noise but it will be too late*" (P7-I). In addition, the majority of participants argued that these devices could result in wrong conclusions being drawn when people raised their voices during an argument or a strike: "*But then there is noise and noise; if you speak too loudly you [might] trigger a false alarm*" (P9-II).

In contrast to the acceptance of sound sensors and video-surveillance, participants felt vulnerable vis-à-vis the collection of their biometric data, in particular DNA, which was perceived as extremely sensitive data since it could reveal information about one's health: "*Biologically speaking, DNA represents the most intimate part of a human being, their [genetic] make-up. Once it has been collected you know the most intimate details about the person, even their illnesses*" (P7-II). Consequently most participants appeared alarmed at the idea of being forced to provide a DNA sample: "*What shocks me is a scenario in which DNA is taken systematically*" (P4-III). Nevertheless, the majority of participants expressed their approval with regards to the collection of criminals' biometric data, since it made them feel safer to know that criminals were registered: "*That is good, when someone goes to jail; I want them to be on file with their DNA*" (P3-II). Additionally, some participants also alluded to the convenient aspect of using biometric technologies in certain situations, such as at the airport: "*I do not think it is such a bad thing, I fly a lot and all these biometric systems save me time*" (P1-I).

For the majority of participants, electronic tagging caused the strongest negative reactions since participants perceived the use of such technology as a tool to control people in their daily life. As mentioned previously, the use of this technology was also regarded as leading to a sense of dehumanisation; in fact, many participants compared the use of electronic tagging for people to the micro-chipping of animals: "*Electronic chips for everyone is tantamount to treating people like cattle*" (P7-I). Some participants also argued that this situation would be akin to slavery: *"[…] you're basically calling for the population to be enslaved"* (P7-II). The constant surveillance of citizens' every move made participants fear the complete loss of their privacy: "*Just think about it, you go to the mall, to the cinema, [...] you would not be able to do anything without people knowing about it. It is appalling*" (P3-III). Specifically the idea of not being able to remove a chip which is implanted into the skin, in contrast to a bracelet which can be more easily removed, seemed to cause uneasiness to most participants: "*You cannot remove it, you are tracked for life*" (P6-I). However, similar to the use of biometric technologies, participants' tolerance for electronic tagging seemed to increase if it was only deployed for specific societal groups, such as for the safety and supervision of children up to a certain age, elderly people and people with mental health issues: "*For people suffering from Alzheimer's disease yes. I would like to be able to find my father*" (P3-II).

With regards to locations of deployment, surveillance was considered as generally acceptable in public places, such as airports, train stations, subways and streets and specifically in areas deemed as dangerous, such as in underground train stations or at car parks. However, participants preferred to be aware of being under surveillance and therefore argued that they should be informed if an area is monitored. On the other hand, the majority of participants strongly rejected surveillance in private areas since this was viewed as a violation of privacy.

5.4 Surveillance Laws and Regulations

During the last part of the focus group sessions the participants discussed two main issues which were the trust participants have in the state and opinions on length of data storage.

5.4.1 Level of trust in the state

The first issue under discussion was the level of trust participants have in the French state. As mentioned previously, in general it appears that the majority of participants trusted the authorities with the collection and use of citizen data. Several participants argued that unless there is a valid and justified cause, citizens are not usually the focus of extensive surveillance: "*[We are monitored] when there is an investigation going on, but otherwise I do not believe we are specifically targeted*" (P4-III). Similarly, participants expressed their trust into the justified and appropriate application of surveillance technologies by secret services: "*[…] they have the means to record us, but they only do it if they have good reasons to*" (P9-I). Thus it appears that the majority of participants were generally not concerned that the state could misuse surveillance data; only a small minority appeared to have a somewhat mistrustful attitude towards the use of their data by the state.

5.4.3 Length of data storage

When discussing length of data storage, more specifically that related to CCTV recordings, participants' opinions about the ideal time period were rather divided. On the one hand, some participants believed that storage length should be as short as possible; in their opinion, if a crime was recorded on CCTV, such data would be requested shortly after the event, and thus they argued that it would be useless to keep such recordings longer than a certain time span. In addition, participants pointed out that the longer the storage time, the higher the risk of misuse of their data. However, on the other hand, some participants were convinced that a longer storage period was essential for crime investigation; in this regard they believed that recordings sometimes could turn out to contain important information only after a longer time period had lapsed: "*If there is an inquiry, they find a 10-year old body, and they found out it was transported in a specific vehicle*" (P7-I). Moreover, one participant alluded to a perceived discrepancy between the storage length of video recordings as required by law and the time taken by the courts so that a court order is issued for surveillance data to be provided as evidence: *"I was assaulted at a cash machine; I reported it to the police. You have to understand that it takes between 1 and 3 months for a judge to order the video to be seized and that banks only keep tapes for 1 to 3 days. There is a mismatch here"* (P7-II).

Participants were generally in favour of a longer storage time of the data belonging to criminals compared to the data of 'ordinary' citizens. Some participants were also in favour of the tracking of ex-convicts charged with violent crimes, in order to prevent possible future crimes: "*For murderers it is a good thing [to continue monitoring their data], to identify repeat offenders*" (P9-II).

6. Conclusion

French participants displayed high awareness that individual citizens are the subjects of surveillance in commercial, boundary, and public spaces. In general, it appears that in these different contexts, video-surveillance was accepted by participants for reasons of national security and personal safety. In business settings, participants were well aware of the commercial motivations behind the use of loyalty cards and in this regard they expressed concerns regarding the sharing of sensitive data with third parties. Concerns about data use and misuse were also raised in relation to the use of smart phones and online services.

Participants' initial reactions to massive integration of data were generally negative. However, upon discussion it appears that the acceptance of dataveillance was contingent on a number of factors including type of data collected, purposes of data collection and use, and whether consent for data sharing was given. Other factors taken into consideration were possible benefits for citizens and risks of data misuse. Overall, participants considered the sharing of a limited amount of basic data to be justified; however, they seemed to prefer the use of their data by the state for administrative and security-related purposes instead of its use for commercial motivations by private companies. Dataveillance was considered as more acceptable when it was perceived as providing certain benefits to citizens, such as an increase in security or a more efficient service for customers.

Overall, several concerns were raised with regards to the use of surveillance, including the possible risks that extensive surveillance poses to the privacy and freedom of citizens, as well as the possibility of misuse of surveillance data. Specifically with regards to the use of smart surveillance, a number of participants expressed mistrust and scepticism vis-à-vis a decision-making process which is fully automated and devoid of human agency. In addition, doubts were raised by most participants in relation to whether surveillance measures actually provide a viable solution for the prevention and reduction of crime; in light of such doubts it appears that participants found it difficult to justify the extensive use of surveillance measures. Therefore, only a minority of participants were in fact willing to sacrifice their privacy for the sake of increased safety in a context of escalating crime. Nevertheless, although participants challenged the notion that surveillance was effective in in relation to crime prevention, the majority of participants appeared to believe that it was useful for crime investigation.

In relation to the acceptance of the different technologically-mediated surveillance tools, whilst video-surveillance and sound sensors appeared to be widely accepted, biometric technologies and electronic tagging, were perceived as intrusive and unacceptable for the surveillance of 'ordinary' citizens since such use was perceived as a means to control citizens. In contrast, most participants appeared to be in favour of the collection of DNA data and the use of electronic tagging for ex-convicts who committed violent crimes.

In general it appears that the majority of participants trusted the authorities with the collection and use of citizen data, with several participants believing that unless there is a valid justification, citizens are not the target of extensive surveillance. Most participants thus appeared unconcerned that the state could

misuse surveillance data. In relation to length of data storage, opinions were rather mixed; while a number of participants appeared to prefer specific limitations of storage times in order to avoid potential misuse of data, others appeared to favour longer storage periods in order to allow access to surveillance data for any future purposes.

In conclusion, the results indicate that the French participants were highly aware of the extent of personal data which is collected by different actors. Most participants questioned whether the extensive use of surveillance could result in higher crime prevention and thus lead to a safer environment for citizens. Nevertheless, a minority of participants did show their readiness to reveal and share personal data if such disclosure resulted in more efficient bureaucratic procedures as well as an increase in personal safety and national security. In general, the use of surveillance technologies appeared to raise concerns amongst participants regarding the risk of data misuse, which overall was considered as a tangible threat.

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

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

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

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

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

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

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

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

- ☐ Yes
- ☐ No

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

- ☐ **Yes**
- ☐ **No**

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

- ☐ Yes
- ☐ No

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

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

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

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

	participant. In order to do this, each of you will be assigned a number, and it is this number that will be used in the report. **I also want to make sure that everyone in the group is comfortable enough to share their opinions. To make this possible, I would like to ask everyone present to follow these ground rules:** ▪ **We would like to hear from everyone in the group - we are interested in everyone's opinion** ▪ **There are no right or wrong answers so let us agree to respect each other's opinions** ▪ **Please make sure that your mobile phones are on silent so that the discussion will not get interrupted** ▪ **It is important that comments are made one at a time, since each participant's opinion is important. So let us agree to not speak at the same time, otherwise it will be difficult for us to capture everything that is said during the discussion** ▪ **Let's agree as a group to respect each other's confidentiality so that everyone feels more comfortable in speaking openly.** **If there is anyone who would like to suggest any other ground rules feel free to put your suggestions forward to the group.** **Does anyone have any questions before we start?** **Ok so let me start off by asking you to briefly introduce yourselves to the group without revealing private information. Let's do a round where you tell us your name and maybe something about you. I will start the round myself... *(carry out a brief personal introduction)*** *Running Total: 10 mi*
Objectives	**Discussion items and exercises**
Word association exercise **[About 5mins]** - *Word-association game serving as an ice-breaker* - *Establish top of mind associations with the key themes* - *Start off the group discussion*	***Item 1*** **First up, we will carry out a short game: I will read out a word and I would like you to say the first couple of things that come to mind when you hear the word. Let's try an example first: What is the first thing that comes to mind if I say the word "*food*"? Preferably, try to think about single words or short phrases, avoiding lengthy descriptions.** *Read Out (one at a time):* *Technology, privacy, national security, personal information, personal safety* ***Running Total: 15min***
Discussion on everyday experiences related	***Item 2*** **Let's talk about something else. I want you to think about instances**

to surveillance

[20min]

- To explore participants' experience with surveillance & how they perceive it

- To explore participants' awareness and knowledge of the different surveillance technologies

during which you feel that either you or your actions are being observed as well as any instances during which you are aware that information about you is being collected. Let's start by thinking about activities you would usually undertake in your everyday life. Let us take the following situations as examples of this.

Scenario 1: Supermarket

As a first example we can take a shopping trip at your usual supermarket. Can you share your thoughts on this?

Scenario 2: Travelling

Let's move on to another situation, this time related to travelling. What about when you travel by air?

Scenario 3: Public place (e.g. museum, stadium)

Now imagine that you are visiting a public place, such as a museum or attending an event such as a sports match or a concert. What kind of activities do you think would be recorded?

Scenario 4: Mobile devices

Let us discuss just one final example. Think about the times you use your mobile phone. What do you think is being recorded in this case?

Aims:

1. Explore the participants' awareness and knowledge of the technologies

2. Explore the participants' experience of being monitored in their many roles

3. Explore the participants' understanding of where their information is ending

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

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

up *4. Explore the participants' views as to why their actions and behaviours are observed, monitored and collected*	***4. <u>Why</u> the information is being recorded, collected and stored:*** ***a. Why do you think your personal information is being recorded and collected?*** ***b. In what ways do you think your personal information will be used?*** ***Running Total: 35min***
Presentation of cards depicting different technologies and applications [10mins] *To expose participants to a selection of relevant SMART technologies & applications in order to enable a better understanding and hence to facilitate the discussion.*	***Item 3*** *Present the following three cards (each depicting a group of different technologies and applications) to the group. The cards will include the following depictions:* ***Card 1 – Person or event recognition & tracking technologies**: Automated moving of closed circuit television (CCTV) cameras; Automatic number plate reader (ANPR) or automatic vehicle number identification (AVNI); and tracking devices such as mobile phone tracking and RFID* ***Card 2 - Biometrics**: Biometric technologies including fingerprint and iris scanning; and automatic facial recognition (AFR)* ***Card 3 - Object and product detection devices**: Knife arches (portal) and X-ray devices* ***Running total: 40min***
Presentation of MIMSI scenario to participants **[30mins]** - *To explore participants' understanding of the implications of MIMSI* - *To explore participants' feelings, beliefs and attitudes vis-à-vis the sharing of personal information*	***Item 4*** *Present the following hypothetical scenario to the group. A recording of the phone conversation can be prepared beforehand and presented to the group.* ***Phone conversation with the Customer Care Agent at the main branch of the Public Employment Service*** ***Customer Care Agent**: Good morning this is Sharon speaking, how are you Mr. Brown? We were expecting your call after your work contract ended over a month ago.* ***Mr. Brown**: Erm...yes in fact that's why I'm calling...* ***Customer Care Agent**: Well, I'm actually not surprised you called now...how was your holiday in Cyprus? I am sure your wife and kids enjoyed the resort you were staying in...*

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

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

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

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

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

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

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

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

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

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

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

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

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

Aims

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

1. Participants' first reactions including:
- Possibility /

1a. How would you feel if this happened to you?

impossibility of scenario
- Acceptability / unacceptability of scenario

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

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

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

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

(Also probe to establish the degree of control / helplessness felt by the participants in such a hypothetical scenario)

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

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

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

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

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

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

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

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

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

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

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

Running Total: 1 hour 15min

Reactions to scenarios

[About 20mins]

- *To stimulate a debate in order to explore the participants' perceptions of the "security vs. privacy trade-off".*

Item 5

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

Due to an significant increase in <u>violent crimes</u> in the capital city, including <u>a spate of kidnappings and murders which seem random and unconnected</u>, the state has decided to introduce CCTV surveillance in every public space, both those publicly owned (such as subways, public gardens and public conveniences) as well as those privately owned (such as shops, malls and taxis) which will enable automated face-recognition. In addition, all the cars passing through the main

- *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*

check points will have their number plates recorded. There are also plans to install sensors in all public areas which are able to detect loud noises such as in the case of someone screaming. All citizens will be required to have their DNA and fingerprints collected, and their iris scanned. The state has also decided that all citizens who are identified as presenting a possible risk to others should be electronically tagged to monitor and track their movements. For their safety, elderly people and children up to the age of 12 years will also be electronically tagged. All the data from these different technologies will be stored in linked databases administered by the police, who will be notified automatically should there be a cause for alarm and risk to any citizen.

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

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

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

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

Aims:

1. Security climate and level of threat

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

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

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

2. Deployment of specific technologies

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

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

2b. Which technologies do you consider <u>invasive</u> and as a

3. Locations of deployment such as: *Airports* *Malls* *Streets* *4. Existence of laws and other safeguards (in relation to the collection, storage and use of data)* *5. Length of storage of surveillance data*	***threat to your privacy? Why?*** ***2c. What do you think of these automated (or semi-automated) technolgies whereby the final decision is taken by the system and not by a human operator?*** ***3a. Which locations do you consider <u>acceptable</u> in relation to being monitored? Why?*** ***3b. Which locations do you consider <u>unacceptable</u> in relation to being monitored?*** ***4a. What do you think about privacy laws? Do they make you feel <u>protected</u>?*** ***4b. Are there any <u>safeguards</u> or conditions that you would find <u>reassuring</u>?*** ***5a. What do you think about the length of storage of surveillance data? Does it make a difference?*** ***To help you probe, provide the following examples to the participants:*** - ***Recordings of CCTV*** - ***The location and movement of cars*** - ***The storage of DNA, fingerprints and iris scans*** - ***The location of citizens who pose a risk to others*** - ***The location and movements of elderly people and children*** ***5b. If length of storage makes a difference, what would you consider as an <u>acceptable timeframe</u>?*** ***Running Total: 1 hour 35min***
Brief summary of discussion [5mins] ▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***Item 6 – Summing up session*** ***At the end of the focus group, it is helpful to provide a summary of the emerging points. Here you should aim at giving a brief summing up of the themes and issues raised during the discussion. After, you can ask for the following from the participants:*** - ***"How well does that capture what was said here today?"*** - ***"Is there anything we have missed?"*** - ***"Did we cover everything?"*** ***This brief session will give participants an additional opportunity to express their views and can also be used to elaborate on topics raised but not pursued at the time.*** ***Running Total: 1 hour 40 min***
Conclusion of focus group **[5mins]** ▪ ***Thank the***	***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**

participants ▪ *Hand out the reimbursement* ▪ *Give information on SMART*	**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 (FRENCH)

Introduction	Briefing
Accueil des participants - *Discours de bienvenue* - *Distribution des badges* - *Signature des formulaires de consentement*	*Accueillir les participants dès leur arrivée. Faire s'asseoir les invités et leur distribuer à chacun leur badge avec leur nom.* *Distribuer les formulaires de consentement, demander aux participants de lire et signer ce formulaire avant la session du groupe de discussion ne commence. Ceci est important afin que les participants sachent à quoi ils se sont engagés.*
Introduction [environ 10 min] - *Remerciements* - *Présentation de l'équipe intervenante* - *Objectifs* - *Confidentialité* - *Durée* - *Règles de base du groupe* - *Bref introduction des participants*	**Bienvenue à ce groupe de discussion, et merci d'avoir accepté notre invitation pour cette session. Nous vous remercions également pour votre implication et pour le temps que vous consacrez à ce projet, malgré vos emplois du temps à tous très chargés.** **Mon nom est _____ et j'animerai ce groupe de discussion. Je serai assisté par _____ mon co-animateur, qui prendra des notes et qui enregistrera notre discussion.** *Présentation des autres collègues qui seront peut être présents* **Notre session durera entre une heure et demie et deux heures. Dans la mesure où nous enregistrerons l'ensemble des discussions, je vous prie de bien vouloir parler de la façon la plus claire possible, vos opinions et vos réflexions sont extrêmement importantes pour cette recherche, et nous ne voudrions pas manquer un seul de vos commentaires.** **Comme nous vous l'avions expliqué précédemment lorsque nous vous avions contactés pour que vous participiez à ce groupe de discussion, le sujet traite de la vie privée et des technologies. Cette discussion s'inscrit dans le cadre du projet SMART, co-fondé avec la union européenne. Pour ceux qui souhaiteraient avoir de plus amples informations sur le projet SMART, n'hésitez pas à nous le faire savoir, afin que nous puissions vous donner plus d'information à la fin de ce groupe de discussion.** *A ce stade, il est important de ne pas divulguer des détails supplémentaires sur le contenu du groupe de discussion afin d'éviter d'influencer et de polariser le débat qui va suivre.* **Comme vous avez pu en être informés suite à la lecture et à la signature du formulaire de consentement, tout ce qui sera enregistré au cours de cette session restera confidentiel et votre identité demeurera anonyme. Cela signifie que vos réflexions ne seront**

	partagées qu'avec ceux qui sont impliqués dans cette étude, elles pourront uniquement être publiées dans les revues scientifiques relatives à cette étude, et ce de façon anonyme. Par conséquent, les informations qui seront incluses dans le rapport ne permettront en aucun cas de vous identifier en tant que participant. Pour ce faire, chacun d'entre vous se verra attribuer un numéro, et c'est ce numéro qui sera ensuite utilisé dans le rapport. **Je tiens également à m'assurer que chacun dans le groupe se sente suffisamment en confiance et à son aise pour pouvoir communiquer son opinion. Pour ce faire, je voudrais demander à toutes les personnes présentes de suivre ces règles de base:** • **Nous aimerions entendre tout le monde dans le groupe - nous sommes intéressés par l'opinion de chacun** • **Il n'y a pas de bonnes ou de mauvaises réponses alors respectons les opinions de chacun** • **S'il vous plaît, assurez-vous que vos téléphones portables soient en mode silencieux afin que la discussion ne soit pas interrompue** • **Il est important que les commentaires soient entendus un par un, car l'opinion de chacun est importante. Alors mettons-nous d'accord pour ne pas parler tous en même temps, sinon ce sera difficile pour nous de retranscrire ensuite l'ensemble de ce qui aura été dit lors de cette discussion.** • **Respectons la confidentialité de chacun, de façon à ce que chacun se sente plus à l'aise et puisse s'exprimer ouvertement.** • **Si l'un d'entre vous souhaite suggérer d'autres règles de fonctionnement pour cette session, n'hésitez pas à nous faire part de vos suggestions.** **Avez-vous des questions avant que nous commencions?** **Ok, permettez-moi de débuter en vous demandant à chacun de vous présenter brièvement sans révéler des informations privées. Nous allons faire un tour de table, vous pourriez dire votre nom et peut être autre chose vous concernant ? Je vais commencer ce tour de table… (Effectuer une brève introduction personnelle)** *Durée totale: 10 min*

Objectifs	Points de discussions et exercices
Jeu d'association de mots **[environ 5min]** - *Jeu d'association*	***Point 1*** *Lecture à voix haute (un à la fois):* *Technologie, vie privée, sécurité nationale, information personnelle,*

de mots afin de briser la glace
- *Etablir des associations d'esprits avec des thèmes clefs*
- *Débuter la discussion de groupe*

sécurité personnelle

Nous allons tout d'abord procéder à un petit jeu: Je vais vous lire un mot et je voudrais que vous me disiez les premières choses qui vous viennent à l'esprit quand vous entendez ce mot. Par exemple: Quelle est la première chose qui vous vient à l'esprit si je prononce le mot «aliments»? Pensez de préférence à des mots ou des phrases courtes, en évitant les longues descriptions.

Durée totale: 15min

Discussion sur l'expérience quotidienne relative à la surveillance

[20min]

- *Comprendre l'experience des participants relative à la surveillance et la manière dont ils la perçoive*

- *Comprendre l'étendue des connaissances et de la sensibilitation des participants sur les technologies de surveillance*

Point 2

Parlons d'autre chose. Je voudrais que vous pensiez à des situations où vous avez senti que soit vous soit vos actions ont été observées. Je voudrais également que vous pensiez à des situations ou vous étiez conscient que des informations vous concernant ont été recueillies. Commençons par réfléchir aux activités que vous entreprenez quotidiennement. Prenons comme exemple les situations qui suivent :

Scenario 1: Super Marché

Le premier exemple c'est lorsque vous faites vos courses au supermarché, quelle est votre opinion sur le sujet ?

Scenario 2: Voyage

La deuxième mise en situation concerne les voyages. Qu'en pensez-vous, notamment lorsque vous prenez l'avion?

Scenario 3: Espace public (ex: musée, stade)

Imaginez à présent que vous visitez un espace public, comme par exemple un musée, ou que vous participez à un évènement sportif ou à un concert. Quels types d'activités à votre avis seraient particulièrement surveillés/enregistrés?

Scenario 4: Téléphonie mobile

Le dernier exemple concerne les moments où vous utilisez votre téléphone portable. Qu'est ce qui selon vous sera enregistré ?

Buts:

1. Comprendre l'étendue des connaissances et de la sensibilisation des participants sur les technologies de surveillance

2. Déterminer

Examiner chaque point suivant en détail quand cela s'avère pertinent.

1. ***Comment l'information est elle colléctée:***

    a. ***Quels types de technologie sont utilisés à votre avis pour collécter vos informations personnelles?***

2. ***Quel type d'information est collecté:***

    b. ***Quel genre d'information personnelle à votre avis est collecté?***

l'expérience qu'à chaque participant dans sa vie de tous les jours lorsqu'il est surveillé

3. Déterminer la compréhension qu'ont les participants sur l'endroit où vont finir ces informations personnelles

3. Qui recueille ces informations:

a. ***Qui à votre avis est responsable pour recueillir et enrregistré l'ensemble de vos informations personnelles ?***

b. ***Où pensez vous que vos informations personnelles vont attérir?***

4. Pourquoi ces informations sont elles enregistrées, recueillies et stockées:

a. ***Pourquoi pensez vous que ces informations sont enregistrées et recueillies?***
b. ***Comment pensez vous que vos informations personnelles seront utilisées?***

4. Comprendre le point de vue de chaque participant sur pourquoi leurs actions et leurs comportements sont observés, surveillés et recueillis

Durée totale: 35min

Présentation des cartes qui décrivent les différentes technologies ainsi que leurs applications [10min]

Présenter aux participants une sélection des technologies SMART pertinentes ainsi que leur application afin d'en améliorer la compréhension et faciliter la discussion.

Point 3

Présentez les trois cartes suivantes (chacune d'entre elle décrivant un groupe de technologie distinct accompagné de son application) les cartes contiennent les descriptions suivantes:

Carte 1 – Reconnaissance d'évènements ou de personnes et technologies de suivi/traçage *: système automatisé de surveillance par télévision en circuit fermé (CCTV) caméras; reconnaissance automatique des plaques d'immatriculation (ANPR) ou système d'identification automatique des véhicules (AVNI); et dispositifs de localisation comme par les téléphones portables et l'identification par radiofréquence RFID*

Carte 2 - Biométrique*: technologies biométriques incluant les empreintes digitales, le balayage de l'iris et la reconnaissance faciale automatique (AFR)*

Carte 3 – Dispositifs de détection des objets et des produits*:*

Détecteurs de métaux Archway et autres dispositifs à rayons X.

Durée totale: 40min

Presentation du MIMSI scenario aux participants

[30min]

- *Déterminer la compréhension des participants sur la MIMSI et son implication*

- *Comprendre les sentiments, les croyances et les attitudes des participants à l'égard du partage des informations personnelles*

Scénario (Partie 4)

Présentez comme suit: scenario hypothétique au groupe . l'enregistrement d'une conversation téléphonique peut être préparé à l'avance et présenté au groupe.

Conversation téléphonique avec un Conseiller d'une agence du Pôle Emploi

***Conseiller** : Bonjour, Sharon à votre écoute, comment-allez vous M. Brown ? Nous étions en attente de votre appel suite à la fin de votre contrat de travail il y a un mois.*

***M. Brown** : Euh… Oui, en effet, et c'est d'ailleurs l'objet de mon appel aujourd'hui…*

***Conseiller** : Très bien, et je ne suis d'ailleurs pas surprise que vous ne nous ayez pas rappelés avant… A ce propos, comment se sont passées vos vacances à Chypre ? Je suis sure que votre femmes et vos enfants ont adoré l'hôtel dans lequel vous avez séjourné…*

***M. Brown** : Oh oui, c'était d'excellentes vacances… mais comment savez-vous tout cela ?*

***Conseiller** : Et bien, c'est enregistré dans notre logiciel, M. Brown… bien évidemment. Bref, maintenant il vaut mieux commencer à chercher un nouvel emploi… étant donné le coût que vont représenter votre séjour en famille et les mensualités pour le crédit de votre voiture… sans parler de vos frais bancaires qui seront prélevés le 22 du mois…*

***M. Brown** : Mais, est-ce que toutes ces informations sont dans votre logiciel également ?*

***Conseiller** : Oui, bien sûr M. Brown. Par ailleurs, vous avez bien fait d'acheter ce livre en ligne... je l'ai lu également et il m'a apporté plein de bons conseils…*

***M. Brown** : Hmmm…ok… mais concernant ce nouveau logiciel pour demandeurs d'emploi, dois-je vous faire parvenir une nouvelle photo plus récente ?*

***Conseiller** : Non, M. Brown, nul besoin, cela est déjà fait ! Nous avons déjà une multitude de nouvelles photos de vous enregistrées dans le système. D'ailleurs, en y repensant… vous aviez très bonne mine avec votre bronzage lors de vos vacances ! Le temps devait être magnifique ! Et avant que j'oublie, pour la photo, vous préférez avec ou sans vos lunettes ?*

***M. Brown** : Euh…. Et bien … sans lunettes plutôt… et pour en revenir à mon inscription, pouvons-nous convenir d'un rendez-vous pour la semaine prochaine ?*

***Conseiller** : Et bien, laissez-moi regarder notre logiciel… Mercredi à midi, cela vous conviendrait-il ? Oh attendez, je viens juste de m'apercevoir que vous aviez déjà un rendez-vous chez le médecin à la même heure ! Et je me doute que vous ne voulez sûrement pas le louper, car c'est important de faire contrôler son taux de cholestérole ! Que dites-vous de jeudi matin à 9 heures ?*

***M. Brown** : Et bien, jeudi matin me convient… dois-je apporter des papiers ou d'autres documents ?*

***Conseiller** : Non cela n'est pas nécessaire M. Brown, nous disposons déjà de toutes les informations dont nous avons besoin dans notre logiciel.*

***M. Brown** : En effet, je n'en doute pas…*

***Conseiller** : Nous vous remercions de votre appel M. Brown, à la semaine prochaine. Et d'ailleurs, bonne dégustation de votre cappuccino au Café Olé…*

***M. Brown** : Oui… merci, c'est déjà fait…. Au revoir…*

Après avoir présenté le scénario précédent au groupe, étudier plus en détail les questions suivantes: gfghfgdf

Buts:

1. Premières réactions des participants, incluant:

Possibilité/Impossibilité des scénarios

Acceptabilité/Non acceptabilité des scénarios

2. Croyances et comportements des participants sur l'effet des technologies sur leur vie privée

1a. Comment vous sentiriez-vous si cela vous arrivait?

(Essayez d'établir le degré de contrôle ou d'impuissance ressenti par les participants dans un tel scénario)

1b. Comment réagiriez-vous si cela vous arrivait ? Que feriez-vous?
1c. Un tel scénario est-il possible/impossible ?
1d. Un tel scénario est-il acceptable/inacceptable?

2a. Dans quelle mesure pensez-vous que les technologies "autonomes" affectent votre vie privée ?

2b. Dans quelle mesure pensez-vous que les technologies intelligentes, par exemple celles qui traitent les données de façon automatique ou semi-automatique, affectent votre vie privée ?

3a. Quel type d'information trouvez-vous acceptable de

3. Croyances et comportements des participants par rapport au type d'information: dossiers médicaux, information financière, photos, localisation

4. Croyances et comportements des participants sur la collecte, l'usage et le partage des informations avec des tiers

5. Croyances et comportements des participants sur les avantages et inconvénients d'être surveillé

collecter, utiliser et/ou partager ?

3b. Quel type d'information refuseriez-vous d'être collecté, utilisé et/ou partagé ?

4a. Que pensez-vous du fait que des données personnes soient collectées, utilisées et partagées par l'Etat ?

4b. Que pensez-vous du fait que des données personnes soient collectées, utilisées et partagées par des entités privées (comme commerciales) ?

5a. Pensez-vous qu'il y a des avantages à ce que vos actions et comportements soient surveillés ?

5b. Pensez-vous qu'il y a des inconvénients à ce que vos actions et comportements soient surveillés ?

Durée totale : 1h15

Réactions aux scénarios (environ 20 min)

- Stimuler un débat pour explorer les perceptions des participants sur le compromis « sécurité vs. Vie privée »
- Ici, la discussion devrait se focaliser sur le fait de savoir si ces technologies augmenteront la sécurité –

Point 5

Pour ce prochain exercice, nous allons discuter des scenarios hypothétiques suivants:

En raison d'une augmentation significative de crimes violents dans la capitale, à savoir une vague d'enlèvements et de meurtres qui ne semblent pas être reliés les uns aux autres, l'Etat a décidé de mettre en place la vidéosurveillance (CCTV) dans l'ensemble des espaces publics, incluant ceux relevant de la propriété publique(métro, jardins publics, toilettes publiques) et ceux relevant de la propriété privée (boutiques, centres commerciaux et taxis), ce qui facilitera la reconnaissance faciale automatique.

En outre, l'ensemble des véhicules qui passent par les principaux points de contrôle auront leurs plaques d'immatriculations enregistrées. Il est également prévu d'installer des capteurs sonores dans tous les espaces publics, qui sont en mesure de détecter des bruits intenses, notamment dans le cas où un individu crierait. On prélèvera l'ADN, les empreintes digitales et on scannera l'iris de l'ensemble des citoyens. L'Etat a également décidé d'étiqueter/ d'enregistrer/ de marquer électroniquement l'ensemble des citoyens

cela devrait être tenu pour acquis. La discussion devrait principalement se focaliser sur le fait de savoir si ces technologies affectent la vie privée et renversent ce compromis	**considérés comme potentiellement dangereux, afin de les surveiller et de pouvoir suivre leurs mouvements. Les personnes âgées et les enfants âgés de moins de 12 ans seront également enregistrés par voie électronique afin de garantir leur sécurité. Toutes les informations collectées par ces différentes technologies seront stockées dans des bases de données administrées par la police, qui seront ensuite notifiés automatiquement en cas de risques encourus par un citoyen.** **Demander aux participants d'imaginer le scénario ci-dessus mais avec les variations suivantes:** **Variation 1: Même si il y a une augmentation significative de la violence et de la criminalité au sein des principales villes voisines, la ville dans laquelle vous résidez ne connaît pas cette évolution. Mais l'Etat décide tout de même d'introduire des dispositifs de surveillance par mesure de précaution.** **Variation 2: L'ensemble du pays connaît des taux de criminalité très bas de manière générale, néanmoins, l'Etat décide tout de même d'introduire des dispositifs de surveillance par mesure de précaution, car une des villes a fait face à un terrible incident aux cours duquel plusieurs personnes ont été tuées et d'autres sévèrement blessées par un homme qui a ouvert le feu dans un centre commercial.** **Pendant la discussion des scénarios/variations ci-dessus, explorez les facteurs suivants en détail et tentez de savoir comment ils peuvent affecter le compromis « sécurité vs. Vie privée » :**
Objectifs: **1. Climat de sécurité et niveau de la menace** **2. Déploiement des technologies**	1a. Dans le scénario, qu'est-ce qui vous fait vous sentir en sécurité ? 1b. Dans le scénario, qu'est-ce qui vous fait vous sentir vulnérable ? 1c. Seriez-vous prêt à sacrifier votre vie privée si le niveau de menace était différent dans les variations 1 et 2 du scénario ? 2. A partir des technologies intelligentes illustrées dans le scénario : Caméras de surveillance avec système de reconnaissance faciale automatisé Reconnaissance de plaques d'immatriculation Capteurs (capacité à détecter des bruits sourds) Technologies biométriques (incluant les empreintes) Marquage électronique 2a. Quelles technologies considérez-vous comme acceptable ? Pourquoi ?

	2b. Quelles technologies considérez-vous comme envahissante et comme une menace pour votre vie privée ? pourquoi ? 2c. Que pensez-vous de ces technologies automatisées ou semi-automatisées pour lesquelles la décision finale est prise par le système et non un opérateur humain ?
3. Emplacement des déploiements comme des aéroports, centres commerciaux, rues	3a. Quels emplacements trouvez-vous acceptables pour être surveillés ? pourquoi ? 3b. Quels emplacements trouvez-vous inacceptables pour être surveillés ?
4. Existence de lois et autres mesures de protection (par rapport à la collecte, l'utilisation et la conservation des données)	4a. Que pensez-vous des lois sur la vie privée ? Vous sentez-vous mieux protégés ? 4b. Y-a-t-il des mesures de protection ou de conditions que vous trouvez rassurants ?
5. Temps de conservation des données	5a. Que pensez-vous du temps de conservation des données ? Cela fait-il une différence ? Pour aider votre sondage, fournissez les exemples suivants aux participants : - Enregistrement des images des caméras - Emplacement et mouvement des voitures - Conservation de l'AND, des empreintes et des captures d'iris - Localisation des citoyens représentant un risque pour les autres - Localisation et mouvement des personnes âgées et des enfants 5b. Si le temps de conservation fait une différence, que considéreriez-vous comme une durée acceptable ?

APPENDIX D – DEBRIEFING FORM

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

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

APPENDIX E – CONSENT FORM

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

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

1.1. Commercial space

1.1.1. Awareness of different surveillance methods/technologies

1.1.1.1. CCTV

1.1.1.2. Loyalty cards

1.1.1.3. Security guards

1.1.2. Perceived purposes

1.1.2.1. Crime-related purposes

1.1.2.1.1. Prevention and investigation of crime

1.1.2.2. Commercial reasons

1.1.2.2.1. Collection of personal data

1.1.2.2.2. Observation of customer buying behavior

1.1.2.2.3. Selling of personal data

1.1.2.2.4. Marketing and advertisement

1.1.2.2.5. Increase sales and customer loyalty

1.1.2.2.6. Creation of profit

1.1.2.2.7. Improve customer service

1.2. Boundary space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. Monitoring of personal data

1.2.1.1.1. Passport and identity check

1.2.1.1.2. Collection of biometric data

1.2.1.1.3. Loyalty cards

1.2.1.1.4. Interrogation by custom's personnel

1.2.1.1.5. Investigation of luggage content

1.2.1.1.6. Body scanners

1.2.2. Perceived purposes

1.2.2.1. National security

1.2.2.1.1. Prevention of crime and terrorism

1.2.2.1.2. Tracking of criminals

1.2.2.2. Passenger safety

1.2.2.3. Collection of data

1.2.2.3.1. Travel habits

1.2.2.4. Custom affairs

1.2.2.5. Monitoring of citizens

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV

1.3.1.2. Television cameras

1.3.1.3. Security guards

1.3.1.4. Bag scanners
1.3.2. Perceived purposes
1.3.2.1. Security
1.3.2.2. Control function
1.3.2.3. Collection of personal data
1.3.2.4. Creation of profiles
1.3.2.5. Protection of property and artefacts
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
1.4.1.3. Monitoring of smart phone applications
1.4.2. Perceived purposes
1.4.2.1. Crime-related purposes
1.4.2.2. Commercial reasons
1.4.2.2.1. Collection of data
1.4.2.2.2. Data sharing
1.4.2.3. Market research

2. Perceptions and attitudes towards smart surveillance and integrated dataveillance
2.1. Feelings
2.1.1. Extreme discomfort
2.1.1.1. Intrusion of privacy
2.1.1.2. Violation of boundaries
2.1.1.3. Helplessness
2.1.2. Indignation and anger
2.1.2.1. Violation of privacy
2.1.3. Disbelief
2.1.3.1. Ignorance
2.1.3.2. Loss of control
2.1.4. Convenience
2.1.4.1. Comfort
2.2. Behavioural intentions
2.2.1. Active reactions
2.2.1.1.1. Take independent action
2.2.1.1.1.1. Defend one's privacy
2.2.1.1.1.2. Change in behaviour
2.2.1.1.1.3. Take legal action
2.2.2. Passive reactions
2.2.2.1. Not concerned
2.2.3. Supportive reactions
2.2.3.1. Contribution to data sharing

2.3. Beliefs
2.3.1. Likelihood of massively integrated dataveillance
2.3.1.1. Availability of data
2.3.1.1.1. Voluntary contribution to the sharing of data
2.3.1.1.2. Inevitability of data sharing
2.3.1.2. Legal aspect
2.3.1.2.1. Restrictions of laws
2.3.2. Acceptance of massively integrated dataveillance
2.3.2.1. Type of data
2.3.2.1.1. Basic data
2.3.2.1.2. Consent
2.3.2.1.3. Relevance of data
2.3.2.2. Loss of control over the spreading of data
2.3.2.2.1. Possible misuse of data
2.3.2.2.2. Security gaps and hackers
2.3.2.2.3. Voluntary contribution
2.3.2.3. Purpose of data collection
2.3.2.3.1. Administrative purposes
2.3.2.3.2. Commercial intentions
2.3.2.3.3. Crime-related purposes and security
2.3.2.3.4. Facilitation of customer convenience and service
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. Reasoning deficiencies
2.3.3.1.2. Mistrust into decision-making of machines
2.3.3.2. Deterrent effect
2.3.3.3. Circumvention of surveillance
2.3.3.4. Effectiveness compared to traditional surveillance

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. Fear
3.1.1.3. Vulnerability and insecurity
3.1.1.4. Indignation
3.1.1.5. Helplessness
3.1.2. General beliefs
3.1.2.1. Violation of rights
3.1.2.2. Instrument for discrimination
3.1.2.3. Threat of data misuse
3.1.2.4. Doubts regarding the use of data only for security purposes

3.1.2.5. Surveillance for criminals only
3.1.2.5.1. Increase of perceived safety
3.1.2.6. Limitation of liberty
3.1.3. Effectiveness of surveillance
3.1.3.1. Surveillance does not result in more security
3.1.3.2. Deterrent effect
3.1.3.3. Crime prevention
3.1.3.4. Crime investigation
3.1.3.5. No solution to crime
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 safety
3.2.1.3. Identification of criminals
3.2.1.4. Misuse
3.2.2. Sound sensors
3.2.2.1. Increase of security for vulnerable groups
3.2.2.2. Inefficiency in crime prevention
3.2.2.3. Wrong conclusions
3.2.3. Biometric data
3.2.3.1. Sensitive data
3.2.3.2. Fear of systematic collection
3.2.3.3. Collection of criminals' DNA
3.2.3.4. Convenient aspect
3.2.4. Electronic tagging (RFID)
3.2.4.1. Control of citizens
3.2.4.2. Dehumanisation
3.2.4.3. Sacrifice of privacy
3.2.4.4. Tracking for life
3.2.4.5. Useful for specific societal groups
3.2.5. Locations of deployment
3.2.5.1. Public spaces
3.2.5.2. Notification of being surveilled
3.2.5.3. Private places

4. Surveillance laws and regulations

4.1. Level of trust in the state
4.1.1. Trust into the current government
4.1.1.1. Appropriate use of surveillance technologies and citizens' data
4.1.2. Mistrust into future governments
4.1.2.1. Change in objectives
4.1.2.2. Possible misuse of data and surveillance technologies

4.2. Transparency of the state’s decision-making

4.2.1.1. Exclusion of citizens’ opinion

4.2.1.2. Perceived helplessness of participants

4.2.1.3. Anti-democratic decision-making

4.2.1.4. Inclusion of citizens into the decision

4.3. Length of data storage

4.3.1.1. Minimization of storage length

4.3.1.2. Risk of data misuse

4.3.1.3. Delayed crime clarification

4.3.1.4. Time restrictions to make use of evidence

4.3.1.5. Longer data storage for criminals