SMART

# Beliefs and attitudes of citizens in Italy towards smart surveillance and privacy

Noellie Brockdorff[1], Christine Garzia[1], Daniele Mezzana[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Laboratory of Citizenship Science, Rome, Italy

November 2013

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

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

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

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

# Table of Contents

1. Key Findings 3
2. Introduction 5
3. Methodology 6
   3.1 Recruitment process 6
   3.2 Discussion guidelines 6
   3.3 Focus group procedure 7
   3.4 Data analysis 7
4. Sample Description 9
5. Results 10
   5.1 Surveillance Technologies in Different Spaces 10
      5.1.1 Commercial space 10
      5.1.2 Boundary space 11
      5.1.3 Common public spaces 11
      5.1.4 Mobile devices and virtual spaces 12
   5.2 Perceptions & Attitudes towards Smart Surveillance and Integrated Dataveillance 14
      5.2.1 Feelings 14
      5.2.2 Behavourial intentions 14
      5.2.3 Beliefs 15
         5.2.3.1 Likelihood of smart surveillance and integrated dataveillance 15
         5.2.3.2 The “invisibility” of surveillance 16
         5.2.3.3 Perceived effectiveness of smart technologies and dataveillance 17
         5.2.3.4 The role of the state 18
   5.3 Security-Privacy Trade-Offs 19
      5.3.1 Acceptance of technological surveillance 19
      5.3.2 Perception of different technologies 20
   5.4 Surveillance Laws & Regulations 22
      5.4.1 A lack of knowledge, information and transparency 22
      5.4.2 Length of data storage 22
6. Conclusion 24

**Acknowledgements** **26**

**Appendices**

A. Recruitment questionnaire 27
B. Interview guidelines (English) 28
C. Interview guidelines (Italian) 39
D. Debriefing form 49
E. Consent form 51
F. Coding map 53

## 1. Key Findings

This document presents the Italian results of a qualitative study undertaken as part of the SMART project – "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727). The analysis and results are based on a set of three focus group discussions comprising of 21 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 Italian participants were overall highly aware that, as citizens, they are subjected to surveillance in different contexts. The findings indicate that surveillance in commercial, boundary and public spaces has undergone a process of normalisation and that in these spaces, technological surveillance was deemed as predominantly acceptable for different reasons, including marketing and security purposes. In contrast, participants felt a sense of unease when discussing surveillance occurring via the use of mobile phones, as well as surveillance taking place in the virtual space. Whilst in relation to mobile devices, this apprehensiveness was mostly due to the perceived ubiquity of surveillance linked to the use of such devices, in the virtual space some participants felt vulnerable due to the permanency of data traces as well as due to the increased likelihood that once data is in the virtual space the risk of misuse is higher.

With regards to the conceptualisation, and understanding, of technology-mediated surveillance, it appears that participants found it easier to conceptualise surveillance methods involving dataveillance and the massive integration of data from different databases rather than surveillance which is automated in nature (smart surveillance). While some participants expressed fascination at the technologies employed for surveillance, at the same time these same participants acknowledged, with a sense of unease, their own lack of understanding of how smart technologies and dataveillance function.

In order to gauge participants' attitudes and beliefs on dataveillance, the group was presented with a fictional scenario illustrating the massive integration of data. After an initial intense reaction to this situation, the participants debated the possibility of dataveillance and massive integration of personal data taking place and proceeded to differentiate between technical and ethical aspects. While from a technological perspective the massive integration of data from different sources was deemed as possible, although probably not to the extent as portrayed in the scenario, from an ethical perspective most participants expressed concerns that such extensive surveillance could be used as a means to control and to have power over citizens. Additionally, other participants mentioned that this type of surveillance could also lead to an invasion of privacy.

For the majority of participants extensive security measures, as depicted in the "security-privacy trade-off" scenario, resulted in feelings of deep insecurity rather than enhancing feelings of personal safety. Albeit privacy concerns were brought up by the participants, the use of surveillance measures revealed even more intensely concerns relating to 'freedom' and 'control'. Nevertheless, a minority of participants stated that they would accept a decrease in privacy for an increase in security.

Participants' opinions differed on the effectiveness of smart surveillance from a security aspect particularly on the autonomous decision-making capabilities of smart technologies. While some participants argued that the judgements taken by automatized systems are more objective, and therefore more precise, others not only challenged this assumption but moreover argued that such systems could erroneously assess or interpret a given situation. Participants holding this second viewpoint appeared to be sceptical and distrustful of technology on its own without human agency and proceeded to argue that technology should be used as a tool which assists the human operator instead of entirely replacing the latter. Additionally, some participants also argued that surveillance should not be regarded as a solution to security-related concerns but advocated alternative options including education.

Different types of surveillance technologies seemed to have varying levels of acceptance. Overall, most participants expressed their acceptance of CCTV and Automated Number Plate Recognition, while, in contrast, the collection of biometric data and electronic tagging caused discomfort and uneasiness amongst the majority of participants. With regards to locations of deployment, surveillance was considered as generally acceptable in public places and in places considered as high risk areas. On the other hand, surveillance was considered as unacceptable in private spaces.

Lastly, it appears that there was a general lack of awareness and knowledge with regards to surveillance laws and regulations. In fact, few participants shared their opinion in relation to current surveillance legislation and those who expressed their thoughts on the matter indicated a sense of mistrust in relation to existing protective measures.

## 2. Introduction

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

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

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

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

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

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

## 3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Overall, 353 participants took part in this research project. All 42 groups had between 6 and 10 participants, excluding 3 groups which had 11, 12 and 13 participants respectively. The focus groups in Italy were carried out on the 18th February, 20th February and 14th March, 2013. The composition of the groups held in Italy is described further on in Section 4.

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

### 3.1 Recruitment process

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

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

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

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

### 3.2 Discussion guidelines

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

The discussion guidelines were translated into each national language where the research was conducted. Moreover, back translations were carried out which entailed an independent translation of the discussion guidelines back into English by a different translator. The back translation was then compared with the original version in order to ensure comparability of meaning and clarify any possible discrepancies. Any possible changes were discussed with the partners, and, where relevant, the necessary amendments were carried out until a final version of the discussion guidelines in the national language was approved. The Italian version of the discussion guidelines can be found in Appendix C.

### 3.3 Focus group procedure

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

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

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

### 3.4 Data analysis

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

Further to the above process, the researchers proceeded to analyse the remaining 11 data sets. Draft versions of each country report were prepared and provided to the respective partner for revision and amendments.

## 4. Description of the Sample

The data analysis for Italy is based on 21 participants since a number of participants dropped out at the last minute and thus could not be replaced. It was noted that, in all age groups, it was rather difficult to find participants willing to attend the focus groups.

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

| Participant number | Group 1 – 18-24 years | Group 2 – 25-44 years | Group 3 – 45+ years |
|---|---|---|---|
| P1 | F | M | F |
| P2 | F | M | F |
| P3 | F | F | F |
| P4 | F | M | F |
| P5 | F | F | F |
| P6 | M | F | M |
| P7 | - | - | F |
| P8 | - | - | F |
| P9 | - | - | M |
| **Total** | **6** | **6** | **9** |

Although there were slight differences in the atmosphere of the three groups, in general the participants were cordial and cooperative, and the discussion was at times rather intense and engaging.

## 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

The pervasiveness of surveillance in commercial spaces was noted throughout this discussion and as stated by one of the participants, *"the consumer is always, in some way, monitored"* (P4-II). The predominant method through which the participants felt surveilled in supermarkets was via loyalty cards, a practice deemed by the participants as being intended mainly for marketing purposes. The majority of participants considered the surveillance of consumer behaviour via loyalty cards as acceptable since it is an "*automatic*" (P9-I) process, and the data gathered is *"not personal"* (P9-III) in the sense that surveillance is perceived as being primarily directed at what is being purchased: *"is it not an observation closely linked to the person, but to me as a consumer"* (P2-II). It seemed that such acceptance also stemmed from the fact that consumers can choose to register for a loyalty card and that consequently, *"consent"* (P6-III) is provided by the consumers themselves: *"However we are aware, we accept this. At a supermarket, in general, if I want the card I give my personal information"* (P4-III). In this case, most participants seemed willing to accept the 'barter' of personal information for future discounts or for the sake of added convenience, whereby for instance particular offers are tailored according to their needs.

On the other hand, a minority of participants expressed rather ambivalent feelings towards surveillance for marketing purposes; as expressed by one of the participants, such a practice is *"quite interesting but also a little unsettling"* (P3-I). Another participant felt more strongly about this type of surveillance, and considered it as a possible "*violation*" since it directs consumers towards particular products.

To a lesser degree, participants also mentioned surveillance via CCTV and payment methods, specifically debit and credit cards. CCTV was mentioned by only a minority of respondents, and, unlike the loyalty card, being subjected to CCTV surveillance was not considered a choice but rather as something out of one's control: "*You have that feeling when you walk into a place and see that there is a camera recording you […] this is against your will. One can know if you were there that day, but all in all it does not bother me at all"* (P4-III). Albeit the participants who mentioned CCTV did feel "*observed*" (P5-II), this surveillance practice was in the main unchallenged and considered acceptable, mostly due to the belief that *"if one has nothing to hide, this is not a problem"* (P6-III).

### 5.1.2 Boundary space

In the context of border control, the discussion specifically focused on an airport setting. In this 'boundary space' the focus group participants mentioned a wide range of surveillance methods and technologies, comprising mainly of an array of biometric surveillance technologies, including fingerprinting, retinal scanning and the biometric passport or electronic identity card, and the monitoring of personal data via passport control, passenger lists or the airline booking system. Mirroring this wide range of methods and technologies is seemingly the participants perception that *"everyone"* (P2-III) is subjected to rigorous attention and scrutiny and that surveillance in this context is much more personal, as well as more meticulous*: "They know everything – who you are, where you live, your phone, everything […] They go to check who you are, what you have done"* (P5-II).

In this space, some of the participants gave the impression that they did conceive of certain elements of smart and integrated surveillance, and, although they did not directly name them as such, these participants did in a rather vague manner allude to the integration of information from the different sources*: "They put all the pieces [of information] together and store them"* (P9-III).

The main purpose identified in this space was national security – in particular the fighting of terrorism and crime. Notwithstanding the belief that such rigorous surveillance practices do result in a *"violation"* (P3-II) of privacy, the majority of participants did not challenge these practices, deeming them as necessary in such a sensitive context and thus as acceptable: "*as a collection of data, this seems to me quite right"* (P5-I). As expressed by one of the participants:

> *"It's true that somehow I feel my privacy violated, however, it is a violation that I feel is good for those who travel, for safety. It is acceptable. Surely they know all the information. But it is an invasion of privacy that, in my judgement, can somehow be tolerated" (P3-II).*

In general, it appeared that in this context the participants felt minimal concern about being under surveillance by a variety of private and public entities, as well as by different national authorities.

### 5.1.3 Common public spaces

In common public spaces such as museums and stadiums where mass events like concerts and sports events are organised, participants mentioned a range of methods through which surveillance occurs, mostly including CCTV and the monitoring of personal data via the purchase of tickets and the registration of membership cards such as the supporters' card for football matches. Some of the participants, rather hesitantly, hinted at certain elements of integrated surveillance, mostly in relation to CCTV with automated face recognition (AFR): *"Probably there are cameras in the stadium, therefore they can associate a face to a name"* (P1-I). Similarly, another participant alluded at their own lack of understanding vis-à-vis the exact operational nature of the surveillance technologies employed:

> *"Now with the new systems all is recorded […] I do not know what technology has been used, because this is also a complex thing. It is not the camera that is on the corner here and records, or the one that is at the post office" (P6-III).*

The above descriptions seem to imply that the recordings from cameras can be checked against databases in order to identify offenders. In fact, one of the main purposes of surveillance mentioned by the participants in this context was the detection and prosecution of crime and violence: *"There are episodes of violence. They just check the people; they record them, even physically, and at the photographic level, those who create disorder"* (P3-II). Some participants additionally mentioned the prevention of crime and violence as another major purpose:

> *"Maybe if there are riots and they arrest you, they ask "What's your name?" And then you are traced to that card, maybe next time measures are taken, for example they forbid you to enter the stadium because you behaved in a certain way"* (P2-II).

In general, the participants found the use of surveillance methods and technologies as acceptable for security-related purposes; as stated by one of the participants: *"[…] as long as this 'violation' occurs inside places like the stadium, to protect the other, to me it is good and can be tolerated"* (P4-II). However, for some participants, this acceptability was contingent on how secure the stored data is: *"If the state police can have these images for security and remain within their walls, it is good, otherwise […]"* (P3-III). In addition, and similarly to the commercial space, acceptance also seemed to stem from the choice involved in frequenting a certain public place: *"If you do not want to be recorded at the stadium just don't go. You can choose: go to the stadium or go to the office, to the bank or elsewhere. You can choose not to go, but you cannot refuse that control"* (P6-III).

In addition, with particular reference to museums, some participants mentioned the use of surveillance for the protection of property and artefacts, while, to a much lesser degree, other participants also mentioned marketing purposes. The latter was specifically related to the purchase of tickets online, whereby for instance, the individual would receive recommendations for other places to visit.

### 5.1.4 Mobile devices and virtual spaces

Within this space, the participants appeared to be rather knowledgeable about the technological surveillance of mobile phone data and the pervasiveness of surveillance; as stated by one of the participants, *"mobile phones have, if desired, a truly infinite capacity for information gathering"* (P5-I). Participants mentioned a range of methods through which technologically mediated surveillance occurs, or can potentially occur, within this context, including the monitoring of call lists, GPS tracking and the recording of conversations. Interestingly, one participant pointed out the role played by the media in helping make certain 'invisible' surveillance practices become 'visible' to the public:

> "*They record everything, even geo positions. This is obvious from the news: when something happens they know exactly at what time, where, which phone was used. We know the*

> *information in this way since at the beginning we were not aware that we are traceable. [But] we are identifiable in everything"* (P3-II)

The perceived purposes differed according to the type of data gathered. Whilst data pertaining to call lists and other information relating to billing systems was mainly understood as surveillance by private commercial operators for economic reasons (marketing and advertising), data obtained from the recording of conversations was understood as surveillance by the state in rather atypical circumstances, mainly those involving legal or political motives. Nevertheless, in relation to the latter type of surveillance, some participants from Group 1 (18-24 years) mentioned a national scandal whereby *"common people"* (P3-I) were subjected to wiretapping. While the participants recounted this incident, the perceived imbalance of power represented by state surveillance (using private surveillance data) was sharply evident.

On a last note, the predominant view in relation to this context was the belief that everyone who uses a mobile device is monitored extensively and that the data stored could eventually be used for surveillance purposes in case *"someone decides to do it"* (P5-I). In relation to this, some participants seemed to convey a general sense of unease, and vulnerability, at the permanency of data traces, expressing concern that some electronic footprints *"remain indelible"* (P4-II) and that their "*'record' remains"* (P3-II).

## 5.2 Perceptions and attitudes towards smart surveillance and integrated dataveillance

One of the central tasks of this study was to research citizens' feelings and beliefs towards smart surveillance and massively integrated dataveillance, the latter referring to "*the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*"[2]. In order to tap into the attitudes of the participants, the group was presented with an everyday scenario: a recorded telephone conversation between a job seeker and a civil servant of the employment agency, where complex surveillance[3] becomes evident.

### 5.2.1 Feelings

After having listened to this conversation, the focus group participants revealed feelings which ranged from 'passive' discomfort, including helplessness, to 'active' anger. Nonetheless, the predominant feeling amongst the different focus groups was an extreme sense of discomfort: described as a *"disturbing"* (P5-I) scenario, this fictitious role play gave rise to an array of feelings including *"anguish"* (P2-III) and *"pure terror"* (P4-II). Such discomfort was also at times felt in physical terms; as described by one of the participants, the scenario elicited *"almost a sense of suffocation"* (P2-I).

When faced with the *"synchronisation"* (P4-II) of the various data portrayed in the scenario, several participants conveyed feelings of helplessness, as exemplified by the comparison made with *"guinea pigs"* (P4-II). Some participants here expressed feelings of resignation – and acceptance – at this *"Big Brother"* (P6-III) depiction: *"What can you do? I can think of absolutely nothing to prevent this"* (P4-III). Only a minority of participants expressed feelings of anger and indignation, mostly due to perceiving such a situation as a violation of human rights.

### 5.2.2 Behavioural intentions

In addition to asking about their feelings upon listening to this conversation, participants were also asked for their resulting behavioural intentions. Mirroring the feelings of discomfort as described above, the predominant reaction amongst participants was passive and seemed to symbolise a 'disconnection' from modern society in some form or another. One participant described how their first impulse would be to become "*a hermit on a mountain*" (P5-I). It seems that such a "physical" withdrawal would in the process reflect a renunciation of technology as a means of communication: *"I would feel very bad in this case, my only wish would be to leave everything and move to the countryside, without ever using any means of electronic communication"* (P4-II). Nevertheless, albeit participants perceived such a

[2] Clarke, R. (1997)

[3] 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.

‘disconnection’ from modern society as the only way to ultimately *“protect”* oneself, it was acknowledged that it is an *“absurd and unrealistic”* (P4-III) way to deal with such a situation.

### 5.2.3 Beliefs

#### 5.2.3.1 Likelihood of smart surveillance and integrated dataveillance

Regarding the likelihood of whether or not smart surveillance and massively integrated dataveillance are possible (currently and/or in the future), the focus group participants in general differentiated mainly between technical and ethical aspects. To a much lesser extent, there was also a brief mention of the legal aspect, whereby a minority of participants argued that “*no organisation has the right to collect this type of information”* (P3-I).

From a technical perspective, the majority of participants considered such as scenario as *“quite possible, maybe not completely”* (P3-II), and, albeit *“unlikely”* (P3-I) to happen at present, most participants perceived the scenario as being *“closer than it seems”* (P2-II). Nevertheless, one participant pointed out that this kind of intrusive surveillance is not a recent phenomenon but one which already existed decades ago, even without the presently available smart methods and technologies:

> *“I think that the technologies of control exist, in the sense that they are far more advanced than what we believe. These controls were in place even 35 years ago, at a time during which there were no social networks and there was still the telephone in tobacco shops. These [controls] were already in place (P6-III).*

Additionally, as argued by another participant, the spread and intensification of surveillance technologies and methods is not merely a technical issue or one which is related to availability of funding; rather, this participant fundamentally perceived this as a matter of ethics:

> *“I think that all these technologies exist and are quite developed and if someone wants to and has the necessary money, tomorrow we will have all this equipment around us. But I think in our Western society, the fact that we are considered as citizens, individuals, people, etc is no longer a matter of privacy, technology, the question is at the ethical level” (P4-I).*

The ethical dimension was mentioned by several other participants and similarly, the most pervasive issue was that the use of such *“special surveillance”* (P3-II) provides a power imbalance which can potentially be used as a means to *“control”* (P3-I) the individual and to *“deprive”* (P3-II) citizens of their freedom. One participant in fact described the system as a “*totalitarian”* one which *“controls all movements for better or worse, all the action”* (P6-I). Other participants underscored the political aspect, pointing out that should a change in the national political scene occur, the use of surveillance, in particular massively integrated dataveillance could increase the vulnerability of citizens:

> "*What worries me the most is to see that if I live in a democracy, albeit imperfect, no problem; but if the things were to turn in different directions, then yes, there would be effective methods of control of everything. This is the danger" (P4-III)*.

A number of participants also expressed concern with regards to the possibility that privacy may be *"violated"* even more by wholly automated surveillance systems since *"a real individual"* (P4-I) is not present. However, while these participants argued that an integrated system as depicted in the scenario would indeed result in a *"restriction of privacy"* (P6-I), it seems that for others the possibility of being controlled was of more concern than any possible breach of privacy:

> *"The problem is that there is nothing wrong in the fact itself that someone has information about me, but the information guarantees you a lot of power. Having that amount of information about me, gives the opportunity to control me or, anyhow, to have power over me" (P3-I)*.

Additionally, some participants in all focus groups, particularly in the younger age group (18-24 years), expressed a strong belief that the likelihood of massively integrated dataveillance taking place would depend to a certain extent on *"the use one makes of technology"* (P5-I). More specifically, here the participants made a reference to an individual's self-responsibility in divulging their personal information; as expressed by one of the participants: *"It's up to you to decide whether to leave some of your data"* (P4-I). The discussion here mainly revolved around self-responsibility in the context of virtual spaces, albeit not exclusively; in fact, some participants made sense of the scenario by linking it to the *"misuse"* or *"thoughtless use"* (P6-I) of social networks, thereby underlining the part played by social networking sites and other online media in the intensification of surveillance. Nevertheless, such an illusion of control via self-censoring was challenged by one participant who argued against such a belief: *"I always thought that by doing that, it is enough, but it is not. I try to protect myself [however I realise that] I am monitored extensively, even though I try to protect myself"* (P3-III). In relation to this, some participants seemed to imply that there is a higher risk of data misuse by private companies, mentioning for instance, the *"sale of databases"* (P7-III), and the potential risks that such misuse could lead to, including *"identity theft"* (P6-III).

#### 5.2.3.2 The "invisibility" of surveillance

Despite the comprehensive information on the different types of smart surveillance technologies and dataveillance methods provided by the focus group moderator prior to the audio-taped scenario, it seems that some participants found difficulty in understanding the exact nature of smart surveillance. In particular, it appears that participants in Group 3 (45+ years) found it difficult to understand the automated nature of smart surveillance and hence in distinguishing the latter from traditional surveillance technologies requiring a human operator at all stages.

On a more general level, it appears that when referring to traditional surveillance technologies, most participants seemed to equate this mostly with CCTV; this might reflect the ubiquitous nature of cameras and the normalisation towards such video surveillance systems. When referring to technology-mediated surveillance, it appears that participants found it easier to conceptualise surveillance methods involving dataveillance and the massive integration of data from different databases, rather than surveillance which is automated in nature (smart surveillance).

With regards to both smart surveillance and massively integrated dataveillance, some participants expressed their fascination at the technologies and methods employed: *"Here they go beyond what we can see, we humble mortals"* (P6-III). This fascination might be linked to the participants' awareness about their apparent lack of knowledge about the said technologies:

> *"We do not know what happens in the machines and this is perhaps the problem. As long as paper records were used, you could burn everything and no trace would be left. But you do not know how things work – because it requires a set of skills that not everybody has: to know what happens behind a computer, how data is managed and everything else"* (P4-II)

In turn, this lack of understanding and "invisibility" of the operational nature of smart technologies and dataveillance methods seems to give rise to a certain apprehension: *"[…] these integrated systems worry me more, because the boundaries [between what is possible or not] are increasingly blurred, you do not see them well"* (P4-II). Along similar lines, some participants also expressed their belief that smart technologies gather data *"indiscriminately"* (P6-I). This contrasts sharply with the perception that traditional surveillance technologies are *"safer"* since their operational nature is less sophisticated and thus better understood; as stated by the same participant, "*you know where their power begins and where it ends"* (P4-II). Nevertheless, some participants did not reveal this fascination vis-à-vis smart surveillance but rather considered the emergence of such methods as a natural outcome of technological advancement, thereby regarding them as "*just objects which have more functions"* (P1-II).

In addition, when referring to massively integrated dataveillance, some participants in Group II (25-44 years) and Group III (45+ years) kept alluding to the permanency of data traces; as stated by one participant, "*[…] everything remains and you can track everything"* (P4-III). Such descriptions seem to suggest that the participants are indeed aware that mass surveillance on a systematic scale takes place in virtual spaces. Described as *"intangible"* data which is dynamic, as opposed to data *"on paper"* (P4-II) which is static, some participants seemingly feel anxiety, as well as suspicion, at being unable to *"take away what has been written"* (P6-II).

### 5.2.3.3 Perceived effectiveness of smart technologies and dataveillance

Issues of effectiveness were also brought up by the participants, whereby effectiveness was discussed through different perspectives. Some participants stated their belief that the sharing of data through smart technologies can be *"very useful"* (P1-II) since such sharing might enhance *"efficiency"* (P4-I), for instance in the case of medical records shared amongst different hospitals. Another issue related to effectiveness which was raised by the participants, primarily in Group I (18-24 years), was the belief that the judgements taken by automatized systems are more *"objective"* (P1-I) and that, by implication, such an assessment is more precise and effective. However, this viewpoint was challenged by the same participants who stated: *"[…] the machine is already set up, and does not have its own judgement. Thus, for some things it can be very helpful and for others not, in my opinion"* (P4-I). In fact, a number of participants expressed their uneasiness at the risk that smart technologies could erroneously assess or interpret a given situation: *"There can always be a mistake produced by a machine"* (P1-I). Such concern seemed to revolve mainly around the possibility that human actions can be *"misunderstood"* (P6-III) and, as a result, the individual would inadvertently be labelled as a 'risk':

> *"About the smart technology, if there is no man, there is a risk that if I make a sudden movement […] and if the technology is not calibrated on certain aspects I can find myself in an unfortunate situation which probably would not arise under human supervision. The machine is not able to assess how a man acts" (P7-III).*

Pondering on the likelihood of a *"false alarm"* (P7-III), a number of participants, mainly from Group III (45+ years) and, to a lesser extent, Group I (18-24 years), argued that a *"machine"* (P1-I) ought not to take the final decision. Instead, smart surveillance should be considered as an aid in decision-making, primarily by *"drawing man's attention"* (P6-III), in order to provide "*a first discernment"* (P9-III) to the human operator. These participants appeared to be sceptical and distrustful of technology on its own without human agency: *"There should be mediation, because if it only sends a signal and then intervenes, there might be times where it really is a false alarm"* (P7-III). These participants seemed keen to challenge the decision-making capabilities of smart technologies, and consequently argued for "*a second further check before a possible intervention"* (P6-III). In addition, it appears that participants in the older age group (45+ years) regarded the use of technology as a last resort, preferring instead an increase in police presence: *"there should be security staff [but] they do not have the policeman to put there, at least as a deterrent. And then you resort to this [technology]"* (P4-III).

#### 5.2.3.4 The role of the state

In addition to the discourse of self-responsibility as described in Section 4.3.3.1 above, at the same time some participants underscored the role, and the responsibility, of the state in guaranteeing and *"protecting"* (P5-II) the privacy of citizens by ensuring a *"correct use of information"* (P4-I). In this regard, while the participants all agreed about the responsibility of the state, they differed in their perceptions with regards the actual "protection" offered by the state. Whereas some declared that their trust in the state is higher than that in private entities, perceiving the state as giving a "*guarantee of quality"* (P1-II), one participant in particular expressed anger due to repeated experiences whereby personal documentation was repeatedly *"lost"* by a public entity: *"So I say to myself: "But how is this possible?" You are the State Police; you should "protect" my privacy"* (P5-II).

## 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 group. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging. The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[4].

When discussing the scenario, the majority of participants had a very intense reaction, perceiving the scenario as being *"absurd"* (P1-I) and *"disturbing"* (P4-I). In contrast, a minority of participants, mainly in Group 2 (25-44 years), deemed the scenario as *"not so extreme"* (P2-II) and *"not so unrealistic"* (P4-II). Overall, rather than enhancing feelings of personal safety, the security measures portrayed in this scenario resulted in feelings of deep insecurity; as stated by one participant: *"This, in theory, should make us feel secure, while in reality it triggers the opposite reaction* (P5-III). A number of participants from the different age groups thus expressed a deep sense of vulnerability and unease: "*I feel caged thinking that whatever I do is recorded, monitored, scanned…the idea of living in a world like this produces more fear than knowing that I find a criminal in my house"* (P5-I). Nevertheless, a minority of participants did allude to the effectiveness of surveillance devices in terms of safety and security; some participants held the belief that smart technologies – referred to as the *"electronic eye"* (P6-I) – are *"more effective"* (P4-III) and that having "*eyes that control"* (P9-III) may serve as a deterrent against crime. It seems that for these participants, the use of smart technologies provided a caring function, thereby providing them with a sense of reassurance and peace of mind: *"However it is better that there are these technologies, because in a place where there are not, anything could happen"* (P1-III). In general, these participants seemed to *"tolerate"* (P2-II) surveillance for security reasons and consequently accepted a decrease in privacy as *"the price to pay for security"* (P4-I).

An aspect which emerged strongly once again during the discussion of the current scenario was the ethical dimension. Albeit the participants perceived such a situation as giving rise to a *"violation of privacy"* (P3-II), the use of surveillance revealed even more intensely concerns relating to "freedom" and "control", which, ultimately, seemed to supersede privacy issues: *"In my opinion it is not even a matter of privacy, it is a matter of freedom"* (P5-I). Such was the perceived violation that one participant in particular could not conceive that anyone would willingly accept to be surveilled in such a manner: *"nobody would accept to be controlled in this way"* (P4-II). Here, the participants expressed uneasiness at living *"in such a world"* (P1-II) where they feel *"limited on a personal level"* (P5-III):

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

> *"I think it would be very unpleasant, as a citizen, having to come to such a thing. I would not like at all the kind of society that would work in this way, where we are supervised all the time. So you are, in practice, no longer master of yourself"* (P4-II).

In certain instances, participants alluded at the ever increasing likelihood, and frustration, of being 'controlled' by a non-human:

> *"Maybe we are heading to this process: the fact that machines completely replace the human element. Somehow we must operate the machines and not that the machines or the technology itself must somehow induce us to do certain things, or command us in a sense" (P5-I).*

Another prevalent belief that emerged in all focus groups was the idea that smart surveillance should not be regarded as a panacea to security-related concerns; in fact a number of participants argued strongly for alternative options "*to curb crime"* (P4-I), with some suggesting that "*other systems for the security of a country"* (P3-III) could be employed, such as education. Consequently, a number of participants challenged the notion that surveillance can, in and of itself, guarantee security. Further to this, others also mentioned the possibility that people will *"find a way"* (P5-I) to circumvent 'the system' by employing methods of neutralisation such as counter-surveillance:

> *"I also agree that this idea of security based on surveillance is still very naïve […] probably it is more convenient because it allows you not to have to deal with a whole set of other issues […] Security associated with surveillance seems to me a way to combat the problems downstream, and therefore, somehow fails […] Once there is this kind of world, one will find ways to contrast these forms of surveillance too" (P1-II).*

Along similar lines, others maintained that rather than escalating to a radical use of surveillance technologies in an effort to increase security and reduce crime, there should be an emphasis on prevention; one which is based on social rather than technological measures. In particular, a number of participants indicated that such measures could be aimed at *"educating people"* (P1-II). As stated by one of the participants: *"I think I would not accept it, perhaps I would organise campaigns more targeted on insecurity, trying to make people more civilised, rather than get to certain extremes: in short, to prevent"* (P4-II). In general, it seems that these participants perceived technologically mediated surveillance as a short-term solution to security related concerns, one which fails to take into consideration the wider picture and long term implications.

### 5.3.2 Perceptions of different technologies

In general, different types of surveillance technologies seemed to meet different levels of acceptance. Overall, the majority of participants in all three focus groups expressed their acceptance of CCTV's and ANPR. In relation to this, some participants highlighted the inconspicuous nature of these particular surveillance technologies as a potential reason for their acceptance:

> *“Probably the cameras in each public place is a system that can be well accepted, at least personally, in the sense that you are being observed but probably you do not even realise that you are being observed by cameras which might be positioned in a spot which makes it less noticeable” (P3-II).*

On the other hand, the gathering of biometric data and electronic tagging – hence surveillance which involves “*the physical sphere”* – were considered as *“an invasion of privacy”* (P3-II). These surveillance practices caused discomfort and uneasiness amongst the majority of participants, particularly the request for a DNA sample, which was deemed as *“most disturbing”* (P4-I) and as a *“radical”* (P3-II) security measure to be taken. This contrasts sharply with the aforementioned technologies which were deemed as much less intrusive due to their potential “invisibility”. In general it seems that the participants strongly rejected the idea of having their bodies reduced to ‘information’ and these practices were deemed as so highly intrusive that some challenged the idea that giving up privacy in this way will actually lead to increased security. Instead, participants seemed to convey a heightened sense of vulnerability in relation to this type of biometric surveillance.

With regards to locations of deployment, surveillance was considered as generally acceptable in public places, such as streets, gardens and parks, and especially in potentially unsafe situations; as expressed by one participant, “w*here there is a danger that something could happen”* (P1-III). Here, participants mentioned surveillance of situations *“where there are many people”* (P5-I) including the organisation of mass events such as demonstrations. Moreover, other participants also indicated their acceptance of surveillance in places considered as high risk areas, such as banks and airports. It appears that in general, surveillance in public places was perceived as part of the ‘caring’ function of surveillance. Nevertheless, there was a minority of participants who did object to being monitored in public spaces: *“I do not like the idea that there is someone watching me in public places, such as parks or places where I can relax”* (P5-I). On the other hand, surveillance was considered as unacceptable in private spaces such as one’s home and dressing rooms in commercial establishments, a space which seems to elicit rather ambivalent feelings:

> *“Even in the dressing rooms in shops, for example. I mean, there I would never like a camera, even if, on the other hand, it is legitimate to see if I steal or not. But my privacy is that, the dressing room is a public place, but it becomes a private place when I want to change there” (P1-I).*

Such an argument aptly portrays one of the central dilemmas of employing surveillance technologies: the sometimes fluid nature of what is regarded by individuals as being a private space and what is in turn considered as a public space.

## 5.4 Surveillance laws and regulations

During the last part of the focus group sessions, the focus shifted to surveillance laws and regulations. A number of issues were discussed, including citizens' awareness of surveillance laws and regulations, views on current legislation and length of data storage of surveillance data.

### 5.4.1 A lack of knowledge, information and transparency

Overall, there appeared to be a lack of awareness in all focus groups with regards to surveillance laws and regulations. While this lack of knowledge seemed particularly evident amongst the participants in Group 2 (25-44 years) and Group 3 (45+ years), it seemed to be less marked in Group 1 (18-24 years) where the younger participants indicated their awareness of specific aspects of the privacy code. In certain instances – and in line with the aspect of self-responsibility mentioned earlier – the participants themselves suggested a lack of knowledge as to which data should be regarded as *"sensitive": "It is obvious that, here too, we should have a clearer idea of what data is right, or mandatory, to provide to public agencies, and which data should remain private"* (P1-II). According to some participants, this lack of knowledge seems to extend even to those who have the authority to manage the personal information of citizens: *"[…] even those who have a responsibility and who manage the information of other people might not have a clear idea of what is right to do and what is wrong, what are the risks, etc"* (P1-II).

In line with the above lack of awareness, very few participants voiced their opinion with regards their view of current surveillance legislation. One participant perceived the legislation as being *"too complicated"* and argued that the laws should be simplified in order to make them *"more accessible and communicable"* (P1-II). Additionally, some participants seemed to indicate a sense of mistrust in relation to existing protective measures: *"I would like a law that would protect me"* (P4-I). Another participant, who also appeared to be rather critical of the existing legal system, argued that surveillance-related law should not *"discriminate"* but should be applied *"in a consistent and uniform way"* (P4-II).

### 5.4.2 Length of data storage

Participants were also asked for their opinions in relation to the length of storage of surveillance data. Once again very few participants expressed their opinion; therefore, it is rather difficult to draw an overall impression. Data from smart CCTV and ANPR was barely addressed by the participants; this might reflect the general acceptance and 'normalisation' towards video surveillance systems. In contrast, the storage of biometric data, mainly DNA, was subject to debate and to different opinions. Although as mentioned earlier the majority of participants objected to the gathering and storage of DNA, some argued that in case this biometric data was requested it should be kept *"for life"* (P6-III). On the other hand, others debated that length of storage of biometric surveillance should be dependent on *"the use of the data"* (P2-III) and that DNA samples should be disposed of once they are no longer needed. In general, this stance appears to reflect the aforementioned discomfort surrounding biometric surveillance.

## 6. Conclusion

Throughout the different focus groups, the Italian participants indicated a high awareness that individual citizens are indeed the subjects of surveillance in the main spaces considered during the discussion. In general, it appears that surveillance in commercial, boundary and public spaces has undergone a process of normalisation, and technologically-mediated surveillance is here considered as mostly acceptable for varying reasons – mainly marketing purposes in relation to the commercial space and security related purposes with respect to boundary and public spaces. On the other hand, the consideration of the virtual space by the participants caused a debate fraught with a sense of unease mostly due to the increased likelihood that data which is *"intangible"* (P4-II) can be easily misused.

With regards to the acceptance of technologically-mediated surveillance, it appears that in general, different types of technologies seemed to meet varying levels of acceptance. To a certain extent, this acceptance seemed contingent on the "visible" or "invisible" nature of the particular surveillance methods and devices. While biometrics and electronic tagging were considered as the least acceptable, mainly due to their invasiveness into the *"physical sphere"* (P3-II), CCTV and ANPR were deemed as mostly acceptable possibly due to their inconspicuous nature. With regards to locations of deployment, the Italian participants deemed surveillance as being generally acceptable in public spaces albeit it was indicated that in particular spaces, the boundaries between what is public and what is private may be rather blurred.

Nevertheless, in the overall context of surveillance, where a lack of understanding vis-à-vis the operational nature of smart technologies was evident, there appeared to be a distinct shift in the feelings and attitudes of the participants. What seemed to be an initial passive reaction, predominantly one of discomfort and withdrawal, turned into one which actively considered the multiple facets of surveillance – the social, political and ethical aspects – and the corresponding ramifications. The power discourse was clear as several participants debated that extensive surveillance causes a loss of freedom and control, and hence results in a sense of vulnerability rather than an increased sense of security. In addition, surveillance-based security was deemed as being a *"naïve"* (P1-II) concept since participants perceived that such a narrow focus does not address the core of the problem. Furthermore, the focus group participants argued that there are countless ways and means to circumvent or neutralise surveillance. Overall, it seems that the Italian participants conveyed scepticism vis-à-vis surveillance-based security.

Lastly, there appeared to be a lack of awareness in all focus groups with regards to surveillance laws and regulations. Some participants appeared to be rather critical of the existing legal system and in particular expressed mistrust in existing protective measures. The desire – and at times demand – for more protection was clearly noticeable:

*There is a famous quote that says: "Who watches the guardians? Who supervises the surveillants?" I think the problem is this: I do not have a problem against it, I think that the problem is to monitor the behaviour of those who have this information about me" (P3-I).*

## 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**<br>- *Greeting participants*<br>- *Provision of name tags*<br>- *Signing of consent forms* | *Welcome the participants as soon as they come in. Assign them a seat and provide them with a name tag.*<br>*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**<br>[about 10 min]<br>- *Thank you*<br>- *Introduction of facilitating team*<br>- *Purpose*<br>- *Confidentiality*<br>- *Duration*<br>- *Ground rules for the group*<br>- *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.**<br>**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.**<br>*Introduce any other colleagues who might also be present*<br>**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.**<br>**As previously mentioned when you were originally contacted to participate in this discussion, this focus group is on the topic of Technology and Privacy, and it is being conducted as part of the SMART Project, which is co-funded by the European Commission. For those of you who wish to know more about the SMART Project, kindly let us know and we will proceed to give you more information at the conclusion of the focus group.**<br>*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.*<br>**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 mins*

| Objectives | Discussion items and exercises |
|---|---|
| Word association exercise<br>[About 5mins] | *Item 1*<br>First up, we will carry out a short game: I will read out a word and I |

| | |
|---|---|
| - *Word-association game serving as an ice-breaker*<br>- *Establish top of mind associations with the key themes*<br>- *Start off the group discussion* | **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.**<br>*Read Out (one at a time):*<br>*Technology, privacy, national security, personal information, personal safety*<br>***Running Total: 15min*** |
| **Discussion on everyday experiences related to surveillance**<br>**[20min]**<br>- *To explore participants' experience with surveillance & how they perceive it*<br>- *To explore participants' awareness and knowledge of the different surveillance technologies*<br>*Aims:* | ***Item 2***<br>**Let's talk about something else. I want you to think about instances during which you feel that either you or your actions are being observed as well as any instances during which you are aware that information about you is being collected. Let's start by thinking about activities you would usually undertake in your everyday life. Let us take the following situations as examples of this.**<br>**Scenario 1: Supermarket**<br>***As a first example we can take a shopping trip at your usual supermarket. Can you share your thoughts on this?***<br>**Scenario 2: Travelling**<br>***Let's move on to another situation, this time related to travelling. What about when you travel by air?***<br>**Scenario 3: Public place (e.g. museum, stadium)**<br>***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?***<br>**Scenario 4: Mobile devices**<br>**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?**<br>*For each item, and where relevant, probe in detail to explore the following:* |

| | |
|---|---|
| *1. Explore the participants' awareness and knowledge of the technologies* | ***1. How is the information being collected:***<br>***a. Which types of technologies do you think are used to collect your personal information?*** |
| *2. Explore the participants' experience of being monitored in their many roles* | ***2. What type of information is being collected:***<br>***a. What type of personal information do you think is being collected?*** |
| *3. Explore the participants' understanding of where their information is ending up* | ***3. Who is collecting the information:***<br>***a. Who do you think is responsible for collecting and recording your personal information?***<br>***b. Where do you think your personal information will end up?*** |
| *4. Explore the participants' views on why their actions and behaviours are observed, monitored and collected* | ***4. Why the information is being recorded, collected and stored:***<br>***a. Why do you think your personal information is being recorded and collected?***<br>***b. In what ways do you think your personal information will be used?***<br>***Running Total: 35min*** |

| | |
|---|---|
| **Presentation of cards depicting different technologies and applications [10mins]**<br>*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***<br>*Present the following three cards (each depicting a group of different technologies and applications) to the group. The cards will include the following depictions:*<br>***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*<br>***Card 2 - Biometrics**: Biometric technologies including fingerprint and iris scanning; and automatic facial recognition (AFR)*<br>***Card 3 - Object and product detection devices**: Knife arches (portal) and X-ray devices*<br>***Running total: 40min*** |
| **Presentation of MIMSI scenario to participants**<br>**[30mins]**<br>- *To explore participants' understanding of the implications of MIMSI*<br>- *To explore participants' feelings, beliefs and attitudes vis-à-vis the sharing of personal information* | ***Item 4***<br>*Present the following hypothetical scenario to the group. A recording of the phone conversation can be prepared beforehand and presented to the group.*<br>***Phone conversation with the Customer Care Agent at the main branch of the Public Employment Service***<br>***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.*<br>***Mr. Brown**: Erm...yes in fact that's why I'm calling...*<br>***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...*<br>***Mr. Brown**: Yes it was a lovely holiday...and how do you know all this?*<br>***Customer Care Agent**: Well, it is in the system, Mr. Brown....obviously. Anyways, better get a head start on finding a new job...what with the cost of your family holiday and your car payment coming up soon...not to mention your VISA payment on the 22nd of this month...* |

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

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

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

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

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

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

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

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

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

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

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

*Aims*

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

*1. Participants' first reactions including:*

*Possibility / impossibility of scenario*

*Acceptability / unacceptability of*

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

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

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

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

| | |
|---|---|
| *scenario* | ***1d. Is such a scenario acceptable / unacceptable?*** |
| *2. Participants' beliefs and attitudes on how technology affects or might affect their privacy* | ***2a. To what extent do you think that "stand alone" (individual technologies) affect your privacy?***<br>***2b. To what extent do you think that "smart technologies" i.e. those which process data in an automatic (or semi-automatic) manner affect your privacy?*** |
| *3. Participants' beliefs and attitudes in terms of the type of information such as: Medical & financial data; photos and location.* | ***3a. What type of personal information do you find acceptable to being collected, used and / or shared?***<br>***3b. What type of personal information would you object to being collected, used and / or shared?*** |
| *4. Participants' beliefs and attitudes on the collection, usage and sharing of personal information with third parties.* | ***4a. What do you think about having your personal information collected, used and shared by the state?***<br>***4b. What do you think about having your personal information collected, used and shared by private entities (such as commercial ones)?*** |
| *5. Participants' beliefs and attitudes on the benefits and drawbacks of being monitored* | ***5a. Do you think there are any benefits to having your actions and behaviour monitored?***<br>***5b. Do you think there are any drawbacks to having your actions and behaviour monitored?***<br>***Running Total: 1 hour 15min*** |
| **Reactions to scenarios**<br>**[About 20mins]**<br>▪ *To stimulate a debate in order to explore the participants' perceptions of the "security vs. privacy trade-off".*<br>▪ *Here, the* | ***Item 5***<br>**During the next exercise, we will be discussing the following hypothetical scenario. Imagine the following scenario:**<br>**Due to an significant increase in *violent crimes* in the capital city, including *a spate of kidnappings and murders which seem random and unconnected*, the state has decided to introduce CCTV surveillance in every public space, both those publicly owned (such as subways, public gardens and public conveniences) as well as those privately owned (such as shops, malls and taxis) which will enable automated face-recognition. In addition, all the cars passing through the main check points will have their number plates recorded. There are also plans to install sensors in all public areas which are able to detect loud** |

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

*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*

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

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

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

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

*Aims:*

*1. Security climate and level of threat*

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

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

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

*2. Deployment of specific technologies*

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

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

***2b. Which technologies do you consider invasive and as a threat to your privacy? Why?***

***2c. What do you think of these automated (or semi-automated) technolgies whereby the final decision is taken by the system and not by a human operator?***

*3. Locations of deployment such as:*
*Airports*
*Malls*
*Streets*

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

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

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

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

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

*5. Length of storage of surveillance data*

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

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

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

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

***Running Total: 1 hour 35min***

| | |
|---|---|
| **Brief summary of discussion**<br>[5mins]<br>▪ *Confirm the main points raised*<br>▪ *Provide a further chance to elaborate on what was said* | ***Item 6 – Summing up session***<br>***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:***<br>- ***"How well does that capture what was said here today?"***<br>- ***"Is there anything we have missed?"***<br>- ***"Did we cover everything?"***<br>-<br>***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.***<br>***Running Total: 1 hour 40 min*** |
| **Conclusion of focus group**<br>**[5mins]**<br>▪ ***Thank the participants***<br>▪ ***Hand out the reimbursement***<br>▪ ***Give information on SMART*** | ***Item 7 –Closure***<br>**With this last exercise our discussion has come to an end. May we take this opportunity to once again thank you for joining us and for sharing your opinions, experiences and thoughts.**<br>***At this point, hand out the reimbursements to the participants and inform the participants about the next steps.***<br>***Give out more information about the SMART to the participants requesting such information.***<br>***Total: 1 hour and 45 min*** |

## APPENDIX C – DISCUSSION GUIDELINES (ITALIAN)

| Introduzione | Sessione informativa |
|---|---|
| **Benvenuto ai partecipanti**<br>*- Saluto ai partecipanti*<br>*- Fornitura dei cartellini con i nomi*<br>*- Firma del modulo sul consenso* | *Saluto di benvenuto ai partecipanti man mano che arrivano. Assegnare loro un posto a sedere e fornire a ciascuno un cartellino con il nome.*<br>*Distribuire il modulo di consenso ai partecipanti e chiedere loro di leggere e firmare il modulo prima dell'inizio del focus group. Questo è importante per assicurarsi che i partecipanti capiscano cosa hanno accettato di fare.* |
| **Introduzione**<br>[10 minuti circa]<br>*- Ringraziamenti*<br>*- Presentazione del facilitating team*<br>*- Finalità*<br>*- Riservatezza*<br>*- Durata*<br>*- Regole di base per il gruppo*<br>*- Breve presentazione dei partecipanti* | **Benvenuti in questo focus group e grazie di aver accettato di partecipare a questa sessione. Apprezziamo il fatto che avete rubato del tempo dai vostri impegni per prendere parte a questo progetto, e la vostra partecipazione è molto apprezzata. Il mio nome è _________________ e io sarò il facilitatore della discussione del gruppo. Sarò assistito da ________________ mio co-moderatore, che prenderà appunti e registrerà la nostra discussione.**<br>*Presentare altri eventuali colleghi presenti*<br>**La sessione durerà tra un'ora e mezza e due ore, e dato che la discussione sarà registrata, vi chiediamo di parlare con voce chiara; le vostre opinioni e i vostri pensieri sono molto importanti per questa ricerca, e non vogliamo perdere nessuna delle vostre osservazioni.**<br>**Come già detto quando siete stati inizialmente contattati per partecipare a questa discussione, il focus group è sul tema del rapporto tra Tecnologia e Privacy, ed è realizzato nell'ambito del progetto SMART, che è co-finanziato dalla Commissione Europea. Quelli di voi che desiderino saperne di più sul progetto SMART, ce lo facciano cortesemente sapere e provvederemo a fornirvi ulteriori informazioni dopo la conclusione del focus group.**<br>*In questa fase è importante non fornire ulteriori dettagli sul contenuto del focus group per evitare di influenzare e polarizzare la discussione che segue.*<br>**Come vi abbiamo già detto quando avete letto e firmato il modulo per il consenso, tutto ciò che verrà registrato durante questa sessione sarà mantenuto riservato e la vostra identità rimarrà anonima.** |

**Questo significa che le vostre osservazioni saranno condivise solo da coloro che sono coinvolti in questo studio e saranno utilizzate in pubblicazioni scientifiche relative a questo studio, e verranno rese anonime prima di essere riportate. Quindi, le informazioni che verranno incluse nella relazione non potranno in alcun modo farvi identificare come partecipanti. Per fare questo, a ciascuno di voi verrà assegnato un numero, ed è questo numero che verrà utilizzato nella relazione.**

**Desidero, inoltre, fare in modo che tutti nel gruppo si sentano sufficientemente a loro agio nel condividere le loro opinioni. Per rendere questo possibile, vorrei chiedere a tutti i presenti di seguire queste regole di base:**

- **Ci piacerebbe ascoltare tutti i partecipanti al gruppo - siamo interessati al parere di ciascuno**

- **Non esistono risposte giuste o sbagliate, pertanto siamo d'accordo a rispettare le rispettive opinioni**

- **Vi prego di accertarvi che i vostri cellulari siano spenti o in modalità silenziosa, in modo che la discussione non venga interrotta**

- **E' importante che i commenti siano fatti uno alla volta, poiché l'opinione di ciascun partecipante conta. Quindi siamo intesi di non parlare in più persone allo stesso tempo, altrimenti sarà difficile per noi cogliere tutto quel che verrà detto durante la discussione**

- **Siamo d'accordo, come gruppo, a rispettare reciprocamente la riservatezza, in modo che ciascuno si senta a suo agio a parlare apertamente.**

**Se c'è qualcuno che desidera suggerire altre regole di base, si senta libero di porre i suoi suggerimenti all'attenzione del gruppo.**

**Qualcuno ha domande da fare prima di cominciare?**

**Bene, dunque vorrei iniziare chiedendovi di presentarvi brevemente al gruppo, senza rivelare informazioni private. Facciamo un giro in cui ci dite il vostro nome e magari qualcosa di voi. Inizierò il giro io stesso**

| | |
|---|---|
| | ..... *(effettuare una breve presentazione personale)*<br>***Totale Aggiornato: 10 min*** |

| Obiettivi | Oggetti di discussione ed esercizi |
|---|---|
| **Esercizio di associazione di parole**<br>**[Circa 5 min]**<br>- *Gioco di associazioni di parole per rompere il ghiaccio*<br>- *Stabilire associazioni spontanee con i temi chiave*<br>- *Cominciare la discussione di gruppo* | ***Oggetto 1***<br>**Per cominciare, faremo un breve gioco: leggerò una parola e vorrei che diceste la prima coppia di cose che vi vengono in mente quando la sentite. Un primo esempio per prova: qual è la prima cosa che vi viene in mente se dico la parola "cibo"? Preferibilmente, provate a pensare a singole parole o brevi frasi, evitando lunghe descrizioni.**<br>*Leggere (una alla volta):*<br>*Tecnologia, privacy, sicurezza nazionale, informazione personale, sicurezza personale*<br>***Totale Aggiornato: 15min*** |
| **Discussione su esperienze quotidiane connesse alla sorveglianza**<br>**[20 min]**<br>- *Per esaminare l'esperienza dei partecipanti circa la sorveglianza e come essi la percepiscono*<br>- *Per esaminare la consapevolezza e la conoscenza dei partecipanti circa le diverse tecnologie della sorveglianza* | ***Oggetto 2***<br>**Parliamo adesso di un'altra cosa. Vorrei che pensiate a casi in cui avete la sensazione che voi o le vostre azioni sono osservate, o a casi in cui vi accorgete che si stanno raccogliendo informazioni su di voi. Cominciamo pensando ad attività che potete svolgere normalmente nella vostra vita di tutti i giorni. Prendiamo come esempi le seguenti situazioni.**<br>**Scenario 1: Supermarket**<br>**Come primo esempio possiamo prendere un giro al vostro supermarket abituale. Potete condividere i vostri pensieri su questo?**<br>**Scenario 2: Viaggiare**<br>**Passiamo ad un'altra situazione, questa volta relativa al viaggiare. Cosa succede quando si viaggia in aereo?**<br>**Scenario 3: Luogo pubblico (es. museo, stadio)**<br>**Ora immaginate di star visitando un luogo pubblico, come un museo, o di partecipare a un evento come un match sportivo o un concerto. Quali a Che tipo di attività pensate che siano registrate?** |

*Obiettivi:*

*1. Esaminare la consapevolezza e la conoscenza delle tecnologie da parte dei partecipanti*

*2. Esaminare l'esperienza che i partecipanti hanno dell'essere monitorati nei loro diversi ruoli*

*3. Esaminare la comprensione che i partecipanti hanno di dove vanno a finire le informazioni che li riguardano*

*4. Esaminare i punti di vista dei partecipanti sul perché le loro azioni e i loro comportamenti sono osservati, monitorizzati e messi insieme*

**Scenario 4: Dispositivi portatili**

**Discutiamo solo un ultimo esempio. Pensate alle volte che usate il telefono cellulare. Cosa ritenete si stia registrando, in questo caso?**

*Per ciascun oggetto, quando rilevante, si sondi in dettaglio per esaminare quanto segue:*

***1. Come le informazioni vengono raccolte:***

***a. Che tipi di tecnologie pensate siano usate per raccogliere i vostri dati personali?***

***2. Che tipo di informazioni vengono raccolte**:*

***a. Che tipo di dati personali pensate vengano raccolte?***

***3. Chi raccoglie le informazioni:***

***a. Chi pensi sia responsabile della raccolta e della registrazione dei tuoi dati personali?***

***b. Dove pensi che i tuoi dat personali vadano a finire?***

*4.* ***Perché i dati sono registrati, messi insieme e immagazzinati:***

***a. Perché pensi che i tuoi dati personali vengono registrati e raccolti?***

***b. In che modo pensi che i tuoi dati personali saranno utilizzati?***

***Totale Aggiornato: 35 min***

| | |
|---|---|
| **Presentazione di carte raffiguranti differenti tecnologie e applicazioni**<br>**[10 min]**<br>*Mostrare ai partecipanti una selezione di importanti tecnologie e applicazioni SMART, in modo da consentire una migliore comprensione e, quindi, per facilitare la discussione.* | ***Oggetto 3***<br>*Presentare le seguenti tre carte (ciascuna raffigurante un gruppo di differenti tecnologie e applicazioni) al gruppo. Le carte includeranno le seguenti descrizioni:*<br>***Carta 1 – Tecnologie di riconoscimento e tracciamento di persone o eventi:*** *Movimento automatico di telecamere di televisioni a circuito chiuso (CCTV); Lettore automatico di numero di targa (ANPR) o identificazione automatica del numero del veicolo (AVNI); e dispositivi di localizzazione quali la tracciabilità del telefono cellulare e la RFID*<br>***Carta 2 - Biometria****: Tecnologie biometriche quali impronte digitali e scansione dell'iride, e riconoscimento automatico del viso (AFR)*<br>***Carta 3 - Dispositivi di rilevazione di oggetti e prodotti****: "Portali coltello" e dispositivi raggi X*<br>***Totale aggiornato: 40min*** |
| **Presentazione dello scenario MIMSI ai partecipanti**<br>**[30min]**<br>- *Per esaminare la comprensione delle implicazioni del MIMSI da parte dei partecipanti*<br>- *Per esaminare i sentimenti, le credenze e le attitudini dei partecipanti circa la condivisione di dati personali* | ***Oggetto 4***<br>*Presentare al gruppo il seguente scenario ipotetico. Va preparata anticipatamente e presentata al gruppo la registrazione di una conversazione telefonica.*<br>***Conversazione telefonica con l'agente di assistenza clienti presso la sede principale del servizio pubblico di collocamento***<br>***Agente assistenza clienti****: Buongiorno sono Maria, come sta sig. Rossi? Ci aspettavamo la sua chiamata dopo che suo contratto di lavoro è terminato, oltre un mese fa.*<br>***Sig. Rossi****: Ehm ... sì, infatti, è per questo che sto chiamando ...*<br>***Agente assistenza clienti****: Beh, io non sono in realtà sorpresa che abbia chiamato ora ... come sono state le vostre vacanze a Cipro? Sono sicuro che a sua moglie e ai suoi bambini è piaciuto il villaggio dove alloggiavate...*<br>***Sig. Rossi****: Sì, è stata una bella vacanza ... e come fa a sapere tutto questo?*<br>***Agente assistenza clienti****: Bene, è nel sistema, sig. Rossi....ovviamente.* |

*Ad ogni modo, è meglio cominciare a capire prima degli altri per trovare un nuovo lavoro... perché ci saranno presto da pagare le spese per le vacanze della sua faiglia e la sua macchina... per non parlare del pagamento della VISA il 22 di questo mese ...*

***Sig. Rossi**: Anche questo è nel vostro sistema?*

***Agente assistenza clienti**: Sì, certo sig. Rossi. A proposito, buona la scelta del libro che ha comprato online ... l'ho letto anch'io e mi ha dato alcuni buoni suggerimenti ...*

***Sig. Rossi**: Hmmm ... ok ... per quanto riguarda questo nuovo servizio di ricerca lavoro, ho bisogno di fornire una mia foto aggiornata?*

***Agente assistenza clienti**: No sig. Rossi, si è già provveduto, naturalmente! Abbiamo un sacco di foto recenti nel nostro sistema. Il che mi ricorda ... bella abbronzatura che ha preso durante il suo soggiorno! Deve aver fatto bel tempo! Prima che mi dimentichi, per quanto riguarda la foto, preferisce una con gli occhiali o una senza?*

***Sig. Rossi**: Oh ... beh .... senza va bene ... quindi per quanto riguarda la mia iscrizione, possiamo fissare un appuntamento per la prossima settimana?*

***Agente assistenza clienti**: Mi faccia controllare il nostro sistema ... che mi dice di mercoledì a mezzogiorno? Oh, aspetti un attimo! Ho appena notato che ha una visita medica in programma proprio in quel momento. E sono sicuro che non la vuole perdere, poiché il monitoraggio del suo livello di colesterolo è sicuramente importante! Che ne dice di giovedì di prima mattina, alle 9?*

***Sig. Rossi**: Giovedì mattina va bene ... ho bisogno di portare della documentazione con me?*

***Agente assistenza clienti**: No sig. Rossi, abbiamo già tutta l'informazione che ci serve nel nostro sistema.*

***Sig. Rossi**: Ne sono certo...*

***Agente assistenza clienti**: Grazie di aver chiamato sig. Rossi, ci vediamo la prossima settimana.  A proposito, si goda il suo capuccino al Caffe*

| | |
|---|---|
| | *Ole'...*<br>***Sig. Rossi**: Sono...arrivederci...*<br>**...** |
| *Obiettivi* | *Dopo aver presentato al gruppo il precedente scenario, andare più in profondità, per analizzare quanto segue:* |
| *1. Prima reazione dei partecipanti, compreso:*<br>*Possibilità / impossibilità dello scenario*<br>*Accettabilità / inaccettabilità dello scenario* | ***1a. Come vi sentireste se questo succedesse a voi?***<br>*(Indagare anche per stabilire il grado di controllo / senso di impotenza provato dai partecipanti rispetto a un tale scenario ipotetico)*<br>***1b. Come reagireste se questo succedesse a voi? Cosa fareste?***<br>***1c. Questo scenario è possibile / impossibile?***<br>***1d. Questo scenario è accettabile / inaccettabile?*** |
| *2. Credenze e attitudini dei partecipanti su come la tecnologia influisce o potrebbe influire sulla loro privacy* | ***2a. In che misura pensate che le tecnologie "indipendenti" (individuali) influiscano sulla vostra privacy?***<br>***2b. In che misura pensate che le "tecnologie smart" (cioè quelle che elaborano dati in modo automatico (o semi-automatico) influiscano sulla vostra privacy?*** |
| *3. Credenze e attitudini dei partecipanti su tipi di dati quali:*<br>*cartelle cliniche;*<br>*informazioni finanziarie;*<br>*foto e localizzazione.* | ***3a. Che tipo di dati personali trovate accettabile che siano raccolti, usati e / o condivisi?***<br>***3b. Su che tipo di dati personali avreste obiezione a che fossero raccolti, usati e / o condivisi?*** |

| | |
|---|---|
| *4. Credenze e attitudini dei partecipanti sulla raccolta, uso e condivisione di dati personali da parte di terzi.*<br>*5. Credenze e attitudini dei partecipanti su benefici e svantaggi dell'essere monitorati* | ***4a. Cosa pensate del fatto che i vostri dati personali siano raccolti, usati e / o condivisi dallo stato?***<br>***4b. Cosa pensate del fatto che i vostri dati personali siano raccolti, usati e / o condivisi da enti privati (ad esempio di tipo commerciale)?***<br>***5a. Pensate ci siano benefici legati al fatto che le vostre azioni e comportamenti siano monitorati?***<br>***5b. Pensate ci siano svantaggi legati al fatto che le vostre azioni e comportamenti siano monitorati?***<br>***Totale aggiornato: 1 ora15min*** |
| **Reazioni agli scenari**<br>**[Circa 20min]**<br>▪ *Per stimolare un dibattito, al fine di esplorare le percezioni dei partecipanti circa il "compromesso sicurezza vs privacy ".*<br>▪ *Qui, la discussione non dovrebbe concentrarsi sull'eventuale aumento di sicurezza causata da queste tecnologie - ciò* | ***Oggetto 5***<br>**Nel corso del prossimo esercizio, discuteremo il seguente scenario ipotetico. Immaginate la seguente situazione:**<br>**A causa di un significativo aumento dei crimini violenti nella capitale, tra cui una ondata di rapimenti e omicidi che sembrano casuali e non collegati tra loro, lo stato ha deciso di introdurre telecamere di sorveglianza in ogni spazio pubblico, sia quelli di proprietà pubblica (ad esempio la metropolitana, giardini pubblici pubblici e gabinetti pubblici) che quelli privati (ad esempio, negozi, centri commerciali e taxi) che consentirà un riconoscimento facciale automatico. Inoltre, le targhe di tutte le auto in transito per i punti di controllo principali saranno registrate. Vi sono anche piani per installare sensori in tutte le aree comuni, che sono in grado di rilevare rumori forti, come quando qualcuno urla. A tutti i cittadini saranno registrati il DNA e le impronte digitali, e sarà scannerizzata l'iride. Lo stato ha inoltre deciso che tutti i cittadini identificati come fonte di possibile rischio per gli altri devono essere etichettati elettronicamente per monitorare e tracciare i loro movimenti. Per la loro sicurezza, anche anziani e bambini fino a 12 anni saranno etichettati elettronicamente. Tutti i dati provenienti da queste diverse tecnologie verranno memorizzati in database collegati tra loro, gestiti dalle forze di polizia, che saranno informate automaticamente nel caso ci dovesse essere un motivo di allarme e di rischio per i cittadini.** |

| | |
|---|---|
| *semmai dovrebbe essere considerato come un dato di fatto. La discussione dovrebbe principalmente centrarsi sulla questione se queste tecnologie riguardino la privacy e, quindi, ruotino attorno al compromesso sicurezza - privacy* | ***Chiedere ai partecipanti di immaginare lo scenario esposto qui sopra, ma con le seguenti variazioni:***<br>**Variazione 1: Anche se nella maggior parte delle città vicine si sta verificando un aumento significativo di crimini violenti, la città dove risiedete non sta sperimentando un aumento della criminalità. Tuttavia lo stato decide comunque di introdurre delle misure di sorveglianza per precauzione.**<br>**Variazione 2: L'intero paese ha un tasso di criminalità molto basso in generale, ma lo stato decide comunque di introdurre misure di sorveglianza per precauzione dopo che in una città vicina si è registrato un incidente isolato, durante il quale un certo numero di persone sono state uccise o gravemente ferite, da un uomo che si è messo a sparare in un centro commerciale.** |
| *Obiettivi:* | *Durante la discussione dello scenario / delle variazioni sopra presentati, sondate per esplorare in dettaglio i seguenti fattori e come essi possono riguardare "il compromesso sicurezza vs privacy":* |
| *1. Clima di sicurezza e livello di minaccia* | ***1a. Cosa vi fa sentire sicuri nello scenario che abbiamo fornito?***<br>***1b. Cosa vi fa sentire vulnerabili nello scenario che abbiamo fornito?***<br>***1c. Sareste disposti a sacrificare la vostra privacy se il livello di minaccia fosse diverso, come nelle variazioni 1 e 2 dello scenario?*** |
| *2. Utilizzazione di specifiche tecnologie* | ***2. Tre le tecnologie intelligenti raffigurate nello scenario, cioè:***<br>***Telecamere a circuito chiuso con riconoscimento facciale automatico***<br>***Riconoscimento auromatico del numero di targa (ANPR),***<br>***Sensori (con la capacità di rilevare rumori forti), Tecnologie biometriche (impronte digitali comprese) e Identificazione elettronica (che utilizza RFID)*** |

| | |
|---|---|
| | ***2a. Quali tecnologie considerate accettabili? Perché?***<br>***2b. Quali tecnologie considerate invasive e come una minaccia alla vostra privacy? Perché?***<br>***2c. Che ne pensate qi queste tecnologie automatiche (o semi-automatiche) , in cui la decisione finale è presa da un sistema e non da un operatore umano?*** |
| *3. Luoghi di “dispiegamento”, ad esempio:*<br>*Aeroporti*<br>*Centri commerciali*<br>*Strade* | ***3a. In quali luoghi considerate accettabile essere monitorati? Perché?***<br>***3b. In quali luoghi considerate inaccettabile essere monitorati? Perché?*** |
| *4. Esistenza di leggi e altre misure di salvaguardia (in relazione alla raccolta, conservazione e uso dei dati)* | ***4a. Cosa pensate delle leggi sulla privacy? Vi fanno sentire protetti?***<br>***4b. Ci sono misure di salvaguardia o condizioni che trovereste rassicuranti?*** |
| *5. Durata della conservazione dei dati legati alla sorveglianza* | ***5a. Cosa pensate della durata della conservazione dei dati legati alla sorveglianza? Fa differenza?***<br>***Per aiutarvi a indagare, fornite i seguenti esempi ai partecipanti:***<br>***Le registrazioni delle telecamere a circuito chiuso***<br>***La posizione e il movimento delle vetture***<br>***La conservazione di DNA, impronte digitali e scansioni dell'iride***<br>***La localizzazione dei cittadini che rappresentano un rischio per gli altri***<br>***La localizzazione ed i movimenti degli anziani e dei bambini***<br>***5b. Se la durata della conservazione fa differenza, quale lasso di tempo considereste accettabile?***<br>***Totale Aggiornato: 1 ora 35min*** |

| | |
|---|---|
| | |
| **Breve riassunto della discussione**<br>[5min]<br>▪ *Confermare i principali punti emersi*<br>*Fornire una ulteriore possibilità di elaborare quanto è stato detto* | *Oggetto 6* **- Sessione ricapitolativa**<br>***Al termine del focus group, è utile fornire una sintesi dei punti emergenti****.* ***A questo punto, si dovrebbe puntare a fornire un breve riassunto dei temi e delle problematiche sollevati nel corso della discussione. Poi, si può chiedere ai partecipanti quanto segue:***<br>***- "In che misura questo coglie ciò che è stato detto qui oggi"***<br>***- "C'è qualcosa che abbiamo perso?"***<br>***- "Abbiamo coperto tutto?"***<br>***Questa breve sessione darà ai partecipanti una opportunità in più per esprimere i loro punti di vista e potrà anche essere usata per elaborare argomenti emersi ma non approfonditi in quel momento.***<br>***Totale aggiornato: 1 ora 40 min*** |
| **Conclusione del focus group**<br>**[5min]**<br>▪ ***Ringraziamenti ai partecipanti***<br>▪ ***Distribuzione dei rimborsi***<br>▪ ***Dare informazioni su SMART*** | ***Oggetto 7 – Chiusura***<br>**Con questo ultimo esercizio la nostra discussione è giunta al termine. Possiamo cogliere questa occasione per ringraziarvi ancora una volta di esservi uniti a noi e di aver condiviso le vostre opinioni, esperienze e riflessioni.**<br>***A questo punto, distribuire i rimborsi ai partecipanti e informare i partecipanti circa i prossimi passi.***<br>***Fornire ulteriori informazioni su SMART ai the participanti che lo richiedono.***<br>***Totale: 1 ora 45 min*** |

## APPENDIX D – DEBRIEFING FORM

| | |
|---|---|
| **SMART WP10**<br>**Focus Group De-briefing form** | |
| **1. Date** | |
| **2. Duration** | |
| **3. Facilitating team** | Moderator:<br>Co-moderator:<br>Other team members: |
| **4. Group composition** | |
| 4a. Number of participants | Participants present: Participant no-shows: |
| 4b. Gender ratio | Males: Females: |
| 4c. Age categories | 18-24 years:<br>25-44 years:<br>45+ years: |
| **5. Overall observations**<br><br>5a. **Group dynamics:** How would you describe the group dynamics / atmosphere during the session?<br><br>5b. **Discussion**: How would you describe the overall flow of the discussion?<br><br>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**<br><br>6a. **Themes:**<br>What were some of the most prominent themes and ideas discussed about?<br><br>Did anything surprising or unexpected emerge (such as new themes and ideas)?<br><br>6b. **Missing information:**<br>Specify any content which you feel was overlooked or not | |

| | |
|---|---|
| explored in detail? (E.g. due to lack of time etc.)<br>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**<br>Did you encounter any difficulties in relation to the following? If yes, kindly explain in detail.<br>7a. **Organisation and logistics** (For instance those relating to location, venue, any interruptions, reimbursement and refreshments)<br>7b. **Time management**: Timing of particular items in the discussion guidelines and timing of the overall discussion<br>7c. **Group facilitation** (For instance whether it was difficult to get the discussion going etc.)<br>7d. **Focus group tools** (For instance the recording equipment and handouts) | |
| **8. Additional comments** | |

## APPENDIX E – CONSENT FORM

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

*Participation*

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

*Confidentiality and anonymity*

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

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

*Data protection and data security*

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

*Risks and benefits*

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

*Questions about the research*

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

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

Signature: Date:

## APPENDIX F – CODING MAP

1. **Surveillance technologies in different spaces**

1.1 Commercial space

1.1.1 Awareness of different surveillance methods/technologies

1.1.1.1 Loyalty cards

1.1.1.2 CCTV

1.1.1.3 Financial monitoring (debit and credit cards)

1.1.2 Perceived purposes

1.1.2.1 Consumer behaviour research and marketing

1.1.2.2 Protection of property and goods

1.2 Boundary (border) space

1.2.1 Awareness of different surveillance methods/technologies

1.2.1.1 Biometric technologies

1.2.1.1.1 Fingerprinting

1.2.1.1.2 Retinal scanning

1.2.1.1.3 Biometric passport

1.2.1.1.4 Electronic identity card

1.2.1.2 Monitoring of personal data

1.2.1.2.1 Passport control

1.2.1.2.2 Passenger lists

1.2.1.2.3 Airline booking systems

1.2.2 Perceived purposes

1.2.2.1 National security

1.3 Common public spaces

1.3.1 Awareness of different surveillance methods/technologies

1.3.1.1 CCTV

1.3.1.2 Monitoring of personal data

1.3.1.2.1 Supporters' card

1.3.2 Perceived purposes

1.3.2.1 Prevention, detection and prosecution of crime

1.3.2.2 Protection of property

1.3.2.3 Marketing

1.4 Mobile devices and virtual spaces

1.4.1 Awareness of different surveillance methods/technologies

1.4.1.1 Monitoring of call lists

1.4.1.2 Location tracking via GPS

1.4.1.3 Recording of conversations (wiretapping)

1.4.2 Perceived purposes

1.4.2.1 Marketing and advertising

1.4.2.2 Legal reasons

1.4.2.3 Political reasons

2. **Perceptions and attitudes towards smart surveillance and dataveillance**

2.1 Feelings

2.1.1 General discomfort

2.1.1.1 Anguish

2.1.1.2 Terror

2.1.2 Physical discomfort

2.1.2.1 Suffocation

2.1.3 Helplessness and resignation

2.1.4 Anger

2.2 Behavioural intentions

2.2.1 Passive reaction

2.2.1.1 Disconnection

2.3 Beliefs

2.3.1 Likelihood of smart surveillance and dataveillance

2.3.1.1 Technical aspect

2.3.1.1.1 Self-responsibility

2.3.1.2 Ethical aspect

2.3.1.2.1 Power imbalance

2.3.1.2.2 Opportunity to control

2.3.1.2.3 Threat to freedom

2.3.1.2.4 Privacy implications

2.3.1.3 Legal aspect

2.3.2 The "invisibility" of surveillance

2.3.2.1 Understanding of smart surveillance and dataveillance

2.3.3 Perceived effectiveness of smart technologies

2.3.3.1 Sharing of data

2.3.3.2 Decision-making capabilities of automatized systems

2.3.4 The role of the state

3. Security-privacy trade-offs

3.1 Acceptance of technological surveillance

3.1.1 Feelings

3.1.1.1 Vulnerability: surveillance produces insecurity

3.1.1.2 Safety and peace of mind: the “caring” function of surveillance
3.1.1.3 Threat to freedom: the “coercive” function of surveillance
3.1.2 General beliefs
3.1.2.1 Ethical dimension
3.1.2.1.1 Violation of privacy and freedom
3.1.2.2 Effectiveness of surveillance
3.1.2.2.1 Effective in deterring crime
3.1.2.2.2 Ineffective in deterring crime
3.1.2.2.3 Alternatives to surveillance (e.g. Education)
3.1.2.2.4 Counter surveillance

3.2 Perceptions of different technologies
3.2.1 CCTV and ANPR
3.2.1.1 Inconspicuous nature of video-surveillance
3.2.2 Biometric data and electronic tagging (RFID)
3.2.2.1 Strong perceptions of bodily/physical invasiveness

3.3 Locations of deployment
3.3.1 Acceptable in public places
3.3.2 Unacceptable in private spaces

4. **Surveillance laws and regulations**

4.1 Feelings and beliefs
4.1.1 Knowledge of legislation
4.1.2 Transparency of legislation
4.1.3 Storage length of surveillance data