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

Noellie Brockdorff[1], Christine Garzia[1], Cristian Bologa[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Universitatea Babes-Bolyai, Cluj-Napoca, Romania

January 2014

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

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

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

Table of Contents

1. Key Findings

This document presents the Romanian 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 20 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 Romanian participants were in general highly aware of being under surveillance in different contexts including the commercial, boundary and public spaces. Participants mentioned a wide range of surveillance technologies and methods pertaining to different spaces, including financial monitoring and the use of loyalty cards to monitor customer behaviour, as well as the use of CCTV systems for the observation of citizens particularly in boundary and public spaces. Overall, participants perceived customer surveillance as taking place for security reasons as well as marketing and advertisement purposes, while they perceived general citizen surveillance as occurring for reasons of national security and personal safety. Most participants were also aware of the extent of surveillance when using a mobile device; in this regard, they perceived such monitoring as occurring for marketing and financial reasons as well as for other functions associated with law enforcement. Nevertheless, although many participants showed a general acceptance of data collection for such purposes, a minority of participants did express concern in relation to how their data might be ultimately used and shared.

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 legal aspects. Even though opinions varied, the majority of participants considered the massive integration of data as being possible from a technical aspect. On the other hand, from a legal perspective, some participants perceived the occurrence of massive integration of data from dataveillance as being unlikely due to legal restrictions. Whilst the acceptability of dataveillance was contingent on a number of factors, the majority of participants were principally against extensive integration of data from dataveillance mainly because it was perceived as a threat to citizens' privacy.

Participants' opinions on the effectiveness of smart surveillance from a security aspect varied, particularly in relation to the autonomous decision-making capabilities of smart technologies. While some participants argued that automatized smart systems are more efficient in comparison to those requiring a human operator, others appeared to be sceptical and distrustful of technology on its own without human agency. These participants disputed the use of fully automated surveillance technologies and instead advocated for the inclusion of the human element in surveillance. Additionally, a minority of participants also argued that surveillance should not be regarded as a solution to security-related concerns but advocated alternative options including education.

During the discussion of the "security-privacy trade off" scenario, it appears that the acceptance of technological surveillance was subject to diverse opinions. While it seems that a number of participants willingly accepted a decrease in privacy for increased personal safety and public security, others expressed a deep sense of vulnerability and unease at the use of invasive surveillance. Not only did these participants perceive the use of surveillance methods as a threat to 'privacy' but, more critically, they perceived this as an attempt by the state to exercise an extreme form of control.

With reference to the participants' perceptions of a number of surveillance technologies, the different types mentioned in the scenario seemed to meet different levels of acceptance. Overall, while most participants expressed their acceptance of CCTV systems, ANPR and sound sensors, the use of biometric technologies and especially location tracking technologies such as electronic tagging provoked strong resistance. Rather than increasing feelings of safety, these surveillance practices caused discomfort and uneasiness amongst the majority of participants, not only due to privacy reasons but most critically due to a loss of control.

Participants were also invited to share their viewpoints on surveillance laws and regulations. Opposing views of the effectiveness of legislation were evident; while some participants regarded current legislation as inadequate, others were rather satisfied with the level of protection offered. Additionally, in relation to the length of storage of surveillance data, expectations were rather varied and while some participants appeared unconcerned regarding storage period, others proceeded to provide a range of different time spans which they perceived as appropriate.

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 Romania is Babes-Bolyai University (BBU).

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

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

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

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

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research project. The focus groups in Romania were carried out on the 18th January, 12th April and 14th May, 2013[2]. The composition of the groups held in Romania is described further on in Section 4.

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

3.1 Recruitment process

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

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

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

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

3.2 Discussion guidelines

[2] The first two groups were conducted prior to the Boston Marathon bombings whilst the last one was carried out after. Nevertheless, it should be noted that there was no significant difference in the attitudes of participants in this group and those of participants in the other two groups.

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

The discussion guidelines were translated into each national language where the research was conducted. Moreover, back translations were carried out which entailed an independent translation of the discussion guidelines back into English by a different translator. The back translation was then compared with the original version in order to ensure comparability of meaning and clarify any possible discrepancies. Any possible changes were discussed with the partners, and, where relevant, the necessary amendments were carried out until a final version of the discussion guidelines in the national language was approved. The Romanian 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 focussed data analysis and drawing together of overarching themes. Thus, the initial coding map was modified as the analysis unfolded. This process of revision was concluded once no new themes emerged and a final coding map was agreed upon. Nevertheless, the emergence of additional lower order codes was not excluded since the analysis of the remaining transcripts was still pending at this stage. The coding map for this report can be found in Appendix F.

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

4. Description of the Sample

The data analysis for Romania is based on 20 participants. In general it was noted that it was rather difficult to find participants willing to attend the different focus groups. Some participants also failed to show up on the day.

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	M	F	M
P2	M	F	F
P3	M	M	No-show
P4	No-show	F	F
P5	M	F	F
P6	M	M	F
P7	M	M	M
P8	F	-	-
Total	**7**	**7**	**6**

The atmosphere in Group 1 (18-24 years) and Group 2 (25-44 years) was described by the moderators as friendly and relaxed and the discussion was considered as rather smooth and free flowing. In contrast, although the atmosphere in Group 3 (45+ years) was cordial, the participants gave the impression that they were suspicious and the discussion was much less flowing. It appears that this was primarily due to the fact that some participants found difficulty in understanding the meaning of some of the questions.

5. Results

5.1 Surveillance Technologies in Different Spaces

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

5.1.1 Commercial space

In the commercial space, specifically in the context of a supermarket, participants in all focus groups generally displayed a high awareness of being surveilled and of having their data collected through different means. The predominant method through which the participants felt surveilled in supermarkets was via CCTV, while other commonly mentioned methods of surveillance included the use of loyalty cards as well as financial monitoring, i.e. the surveillance of debit or credit card movements. To a much lesser extent, participants mentioned other means of surveillance, including the use of theft detection devices.

The perceived purposes of surveillance tools differed according to the methods in question. In general, it appears that CCTV systems have been widely accepted as a standard surveillance tool in supermarkets and the majority of participants perceived video-surveillance as being used primarily for security reasons, particularly for the investigation of *"thefts and burglary"* (P5-I). Additionally, one participant perceived CCTV systems as possibly also having a preventive function: *"[…] in order to identify thieves or persons who are entering the store and have committed offenses in that store in the past"* (P2-1). Another reason mentioned in relation to video-surveillance was the monitoring of employees in order "*to check whether they are doing their jobs right"* (P5-III). Nevertheless, although widely accepted, some participants emphasised that their acceptance of CCTV systems was contingent on such surveillance being used strictly for security-related purposes: *"I don't mind video-surveillance as long as it is not used for other purposes"* (P3-II).

The collection of data in relation to consumer patterns such as *"the quantity purchased, the quality of products and their price"* (P4-III) was perceived as being collected for the purpose of creating customer databases. This data was considered as having various purposes including those related to sales optimisation, advertising and market research. Moreover a minority of participants perceived the collection of such a vast amount of data as being highly lucrative: *"This data is valuable, they can easily sell it"* (P2-I).

Lastly, it appears that some participants did not exclude other possible covert motives for surveillance in a commercial context; as stated by one participant, *"I don't know any other reasons; perhaps there might be hidden reasons which are so well hidden that I don't know about them"* (P7-I).

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. The use of video-surveillance, including smart CCTV with automatic facial recognition (AFR), and different biometric technologies, including fingerprinting, retinal and iris scanning was perceived as being prevalent in this context. Participants also mentioned a number of object and product detection devices, such as luggage controls, metal detectors and full body scanners as well as the monitoring of personal data via passport control, passenger lists or the airline booking system. In addition, it appears that participants were generally aware of being surveilled by a variety of other entities, including flight companies and a number of national authorities such as the Border Police.

In this context, participants perceived national security and traveller safety as the major purposes of surveillance. In particular, participants mentioned the prevention of crimes by the prior identification of criminals or dangerous suspects, especially those linked to terrorism, although not exclusively. Participants also mentioned the possibility that such surveillance can also be used as a means to control national borders, for instance in order to detect individuals who are prohibited from leaving the country.

Although the majority of participants clearly declared their acceptance of surveillance measures in such a sensitive context, *"[…] I accept all control steps as simple formalities that I respect and consider necessary"* (P5-II), some participants expressed unease at the scrutiny they are subjected to in airports: *"I feel uncomfortable towards all security measures in airports; they make you feel guilty even if you are not"* (P1-II).

5.1.3 Common public spaces

In common public places, such as stadiums where mass events are organised, CCTV was perceived as the predominant surveillance technology used by security personnel and law enforcement officers, mainly for visitor safety and protection of property as well as general security reasons. In addition to the conventional CCTV, participants also alluded to the use of smart CCTV with automatic facial recognition (AFR). Such technology was perceived as monitoring different kinds of personal data including the analysis of facial features as well as the observation of behaviour and gestures.

Video-surveillance data was regarded as having several purposes, including the prevention of crime and violence. As a case in point, participants mentioned the timely identification of known or suspected hooligans: *"[…] to prevent access to those who have been banned from entering the stadium"* (P3-I). Other purposes mentioned were the detection of incidents, so that security personnel or law

enforcement officers are able to intervene in a timely manner, as well as the investigation of incidents. Additionally, the use of video surveillance was regarded as a tool for crowd monitoring and for the regulation of visitor flow.

To a lesser degree, other security measures mentioned by the participants included the use of object detection devices and microphones. Surveillance in this context, specifically for sports events, was perceived by some participants as also occurring via the collection of personal data, including name and address, when purchasing tickets for the events.

5.1.4 Mobile devices

The participants from Group 1 (18-24 years) and Group 2 (25-44 years)[3] were generally aware about the extent of surveillance when making use of a mobile device; as stated by one of the participants, *"[…] the data provided by mobile devices is so extensive that you can find almost anything about the owner"* (P2-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, location tracking through GPS and the recording of conversations. Significantly fewer participants mentioned the collection of data through smart phone applications.

The perceived purposes differed according to the type of data gathered. Data pertaining to call lists and other information relating to billing systems was mainly understood as surveillance by the mobile phone provider for marketing and financial reasons. On the other hand, specifically in relation to the recording of conversations, it seems that while some participants had the impression that all conversations are actually recorded, several others perceived such recording as occurring only in certain circumstances, most notably in cases of suspected illegal activity. The participants perceived such *"special cases"* (P1-I) as requiring a warrant: *"[…] the police [can obtain the recordings of phone conversations] if they have a court order to conduct certain investigations"* (P3-I). Different functions of this type of surveillance were perceived by the participants. Firstly, participants mentioned surveillance for reasons of crime prevention: *"to detect a potential danger"* (P6-II), as well as for reasons of crime detection, including fraud and drug trafficking: *"[…] it is very easy to catch a group of drug dealers if you have a record of the conversations"* (P7-I). Moreover, such monitoring was additionally perceived as a way of obtaining evidence for criminal investigations and prosecution*: "For evidence in case of illegal activities"* (P4-II). To a lesser extent, such purposes were also perceived as being pertinent to location tracking via GPS.

Lastly, in relation to where the data collected ends up, participants were highly aware that the data collected by the mobile phone provider can be potentially shared with several third parties, mainly with marketing companies and the authorities, including the police, the Romanian Intelligence Service (SRI) as well as other foreign intelligent agencies. In relation to this, one participant pointed out the role played by the media in helping make certain 'invisible' surveillance practices become 'visible' to the

[3] This topic was not addressed during Group 3 (45+ years).

public: *“[…] we have explicit examples from television where data are going outside the service supplier; the data could go in several directions, [for instance] to the authorities”* (P2-I).

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"*[4]. In order to elicit the attitudes of the participants, the group was presented with an everyday scenario: a recorded telephone conversation between a job seeker and a civil servant of the employment agency, where complex surveillance[5] becomes evident.

5.2.1 Feelings

After having listened to this conversation, the focus group participants revealed feelings which predominantly indicated an extreme sense of discomfort.; comparing this to a "*big brother*" (P2-I) scenario due to the perception of being "*watched all the time*" (P3-I), the participants expressed a range of feelings which included feeling *"fenced"* (P8-I), *"shocked"* (P2-II), *"exposed"* (P6-II) and *"miserable"* (P4-III).

It seems that these participants were so perturbed that they simply could not conceive of such a situation: *"I cannot imagine myself in this situation, I don't know, I think I would be speechless"* (P7-I). Another participant similarly expressed this unreal feeling, likening it to *"[being] on a TV show"* (P7-II). Significantly fewer participants, predominantly from Group 1 (18-24 years) and some participants from Group 3 (45+ years), experienced indignation, outrage and anger at such a perceived violation of privacy: *"I would be pissed off"* (P4-III).

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. The majority of participants, mainly from Group 2 (25-44 years) and Group 3 (45+ years), suggested a rather passive reaction involving some kind of immediate withdrawal from the hypothetical situation, such as hanging up the phone: *"I would get off the phone very quickly"* (P1-II). Similarly, a minority of participants appeared to experience a sense of helplessness and resignation at such a situation: "*I don't think anything can be done, [I would feel like] I can't do anything*" (P1-I).

On the other hand, other participants stated they would engage in different behaviours in order to counteract such a situation. In this regard, several members of Group 1 (18-24 years) claimed they would resort to legal action: *"I think I would file a lawsuit in the worst case [scenario]"* (P2-I) while other

[4] Clarke, R. (1997)

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

participants argued they would personally investigate how such personal information was obtained: *"I would get informed about the way they collect information about my private life"* (P4-II).

5.2.3 Beliefs

5.2.3.1 Likelihood of integrated dataveillance

Regarding the likelihood of whether or not massively integrated dataveillance is possible (currently and/or in the future), the respondents in general differentiated mainly between technical and legal aspects. Although opinions varied, it appears that the majority of participants regarded the development of massively integrated dataveillance as possible from a technical aspect. As pointed out by one of the participants, all the information is available; what is needed is the technical capacity to *"assemble it all in one place"* (P3-I). Nevertheless, others could not conceive of such technical capabilities: *"I believe it's impossible to have so much data"* (P2-III). Moreover, some participants argued that the massive integration of data is not currently possible due to legal restrictions: *"At the moment I do not think that anyone is allowed to access so much information about you"* (P2-I).

Some participants expressed a strong belief that the likelihood of massively integrated dataveillance taking place would depend to a certain extent on the individual's self-responsibility in divulging their personal information; as expressed by one of the participants: *"It depends. It might be possible if we did not pay attention and sign all sorts of contracts and we spread [our] personal data in a thousand places"* (P3-I). Moreover, it seems that some participants made sense of the scenario by linking it to the use, or rather misuse, of social networks: *"It affects my privacy as much as I allow it to. If I don't wish to give out my location and my activities, I won't post anything about them on social networks"* (P2-II).

5.2.3.2 Acceptance of integrated dataveillance

After discussing the likelihood of massively integrated dataveillance, the participants also discussed its acceptability. Perceiving this situation as an *"invasion of privacy"* (P5-II), an overwhelming majority of participants regarded the scenario as clearly unacceptable: *"It is not alright for others to know all my personal information"* (P1-II). It appears that participants' acceptance of dataveillance depended on a number of factors, including whether consent was explicitly provided by the citizen, *"Without consent none of this would be acceptable"* (P2-I). Another matter which had a bearing on the acceptance of dataveillance was the issue of which entity would have access to such data. Firstly, most participants considered data collection, usage and sharing by the state as generally acceptable, and, in certain cases as necessary, with only a minority of participants, mostly from Group 3 (45+ years), objecting to it. On the other hand, a clear majority of participants categorically opposed the collection, use and sharing of data by private entities: *"[…] but in case of private businesses, many times, the way they get into your private life, to advertise and sell their products, to me it seems abusive"* (P4-II). Overall, the participants expressed a lack of trust in private entities. Additionally, the remaining participants stated that they

would accept this only on condition of anonymity, i.e. that the data cannot be traced back to the person: *"Regarding the private sector, I agree with the use of my personal information for research and statistics [purposes], unless this exposes the person in question"* (P7-II).

The acceptance of dataveillance also depended on the type of data to be stored and shared. Although there were slight differences in the opinions of participants, some general trends emerged. The storage and sharing of personal data such as name, age and gender (i.e. data available on one's identity card) as well as personal data relating to one's profession was generally considered as acceptable. On the other hand, the storage and sharing of other data such as home address, e-mail-address and photos was less accepted. Data considered as most sensitive and thus as extremely confidential included social security details, financial information as well as medical and health data. Nevertheless, in relation to medical and health data, it appears that some participants appreciated the utility of storing and sharing this type of sensitive data, which could be life-saving in cases of medical emergencies. Lastly, it appears that a major concern for some participants in relation to the sharing of data was the possibility that their personal data could somehow be leaked: *"they can become public"* (P4-II).

5.2.3.3 Perceived effectiveness of smart surveillance and dataveillance

Issues of effectiveness of smart surveillance and dataveillance were discussed from various perspectives. Firstly, the issue of automation brought up mixed feelings and varying beliefs amongst the participants. Some participants argued that automatized systems are considerably superior to technologies requiring a human operator, since *"they considerably exceed human capacity, especially since human operators are not always well-trained. A very good computer programme far exceeds the human mind"* (P2-I). These participants maintained that the use of smart technologies has several advantages, including the likelihood that less errors are made. Moreover, they argued that the use of smart surveillance is more efficient in relation to the timely investigation and solving of crimes.

On the other hand, a number of participants, predominantly from Group 2 (25-44 years) and Group 3 (45+ years), appeared sceptical and distrustful of technology on its own without human agency. The findings also suggest that some participants, especially those pertaining to the 45+ age group, found it particularly difficult to understand the exact nature of smart surveillance: *"Effectively, we really do not know anything about them [smart technologies], now I heard about them for the first time"* (P4-III). In turn, this lack of understanding could have had a bearing on their attitudes. In general, participants from these two groups challenged the decision-making capabilities of smart technologies and in particular seemed concerned about the possibility that wrong interpretations could be made by the system. Perceiving the use of automatized systems as *"stealing the right to human judgement [and] free will"* (P6-II), one participant argued that their use leads to a sense of dehumanisation. In line with this, these participants disputed the use of fully automated surveillance technologies and instead advocated for the inclusion of the human element in the surveillance process: *"I disagree with automated decisions. A person has to handle the case to see what happened"* (P6-III). Here, the participants perceived the role of humans as being one of *"supervision and control"* (P5-II). In particular, some participants emphasised

that a *"machine"* ought not to take the final decision but that there should be *"subsequent verification by specialised personnel"* (P7-III) in this regard.

On a last note, notwithstanding this debate about the pros and cons of automation, one participant did emphasise that neither human, nor technological intervention is ultimately infallible: *"Given the fact that it is a machine, it can make errors. But man can also fail"* (P5-III).

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[6].

When discussing the scenario, the acceptance of technological surveillance was subject to different opinions and debated from a range of perspectives. Firstly, some participants regarded the implementation of the aforementioned security measures as having the potential to increase personal safety and public security through different ways, such as providing law enforcement personnel the opportunity to *"anticipate criminal moves"* (P1-II). In general, due to this perception, it appears that these participants were willing to accept a decrease in privacy for increased safety and security: *"From my point of view, it is worth sacrificing privacy"* (P1-III). Nevertheless, while these participants seemingly conveyed their acceptance in a rather unhesitant manner, others appeared to emphasise that such acceptance was not unconditional: *"[…] as long as they are used for protecting citizens […] it depends on the purpose of their use. As long as they are used by the police, or the state, to help citizens, it wouldn't bother me"* (P4-II). It seems that for these participants, the use of technological surveillance by the state provided a caring function, thereby providing them with a sense of reassurance and peace of mind. Nevertheless, other participants challenged whether technologically-mediated surveillance would be effective in offering actual protection to citizens. As a case in point, one participant specifically questioned, rather mockingly, the utility of video-surveillance:

> *"What would make me feel safe if I have already been shot? Certainly the camera won't jump on him [the aggressor] or it won't stop the bullets […] it doesn't help me. It doesn't help with anything, honestly"* (P1-I).

Another belief that emerged from a minority of participants was the idea that surveillance should not be regarded as a panacea for security-related concerns. These participants suggested that *"there are other ways to prevent various situations"* (P4-II); in particular, one participant argued that *"education should completely replace these systems"* (P2-I).

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

Others expressed a deep sense of vulnerability and unease at the use of such invasive surveillance: *"Nothing makes me feel safe, on the contrary"* (P4-III). These participants voiced a number of concerns and debated the use of surveillance from an ethical standpoint. In particular, they appeared concerned that the focus of surveillance could shift from monitoring criminals to observing all citizens. Consequently, they argued that the intensification of surveillance could result in a general criminalisation of citizens: "*I think the use of these technologies is exaggerated and would give me the impression that somebody considers me a criminal"* (P7-II). As similarly stated by another participant, *"[…] it means everyone is a criminal from the outset"* (P5-III), thereby leading to a potential situation where normal citizens feel *"persecuted and followed"* (P2-II). Additionally, not only did these participants perceive the use of surveillance methods as a threat to privacy but, more critically, as an attempt by the state to exercise an extreme form of control:

> *"They will violate my privacy from the moment in which all this will be applied and ratified by the state; the state will become a police state in which all the population will be tracked and monitored. I don't like this (P4-III).*

Similarly, another participant highlighted the controlling function of surveillance, perceiving technology as a tool which helps to satisfy a deep-seated desire to control others: *"they [surveillance technologies] are a manifestation of the human pattern in controlling, in wanting to observe anything that happens"* (P2-I).

In addition to the ethical concerns mentioned above, other concerns of a more technological nature seemed to contribute to the participants' feelings of vulnerability. Firstly, some participants mentioned the possibility that digital evidence can somehow be manipulated, potentially resulting in circumstances where an individual is *"incriminated unjustly"* (P7-II). Secondly, as mentioned previously in relation to dataveillance, other participants appeared concerned at the possibility that stored data could be leaked: *"I wouldn't feel safe if the recordings end up in someone else's hands"* (P4-II).

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 Smart CCTV's, ANPR and sound sensors, albeit a number of participants did express their reservations in relation to these technologies. Video-surveillance was generally considered as *"minimally invasive"* (P1-II) most probably due to its inconspicuous nature: *"As long as you don't know about it at all, it doesn't affect your privacy"* (P4-III). Nevertheless, a minority of participants did object to the use of video-surveillance mainly due to privacy reasons; one participant was particularly concerned that the use of such systems could facilitate the investigation of a person's habits and lifestyle patterns: *"I assume that [cameras] store not only faces but also their movements; I went there, I did that and that, so I guess [also] a chain of events"* (P1-I).

On the other hand, the collection of biometric data and especially the use of electronic tagging devices were considered as invasive practices, and, consequently, the majority of participants considered this type of surveillance as unacceptable. In general, it appears that the participants strongly rejected the idea of having their *"biological features"* (P6-II) reduced to 'information'. These surveillance practices caused discomfort and uneasiness amongst the majority of participants. In particular, the use of electronic tagging was considered as being extremely intrusive and was thus considered as downright unacceptable, *"[…] we are not products in order to be tagged"* (P3-I). A substantial majority of participants objected to the use of electronic tagging devices on ethical grounds, mostly perceiving the use of such technology as providing a means to control others and thus as presenting a threat to citizens' freedom:

> *"I do not agree with the electronic tagging of myself and other persons. Maybe this could lead to situations where someone tells us what to do, just like a remote control […] maybe you can be given orders" (P5-III).*

With regards to locations of deployment, surveillance was considered as generally acceptable in public places, such as streets and train stations, and in privately-owned private spaces frequented by the public, such as shops. Surveillance was also regarded as acceptable in potentially unsafe situations where "*unpleasant incidents can take place"* (P6-II) including places were large crowds gather, such as in stadiums. 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 such public places was perceived as part of the 'caring' function of surveillance.

To a certain extent, participants' acceptance of surveillance in public spaces seemed to stem from the perception that in public places, surveillance is not specifically directed at anyone in particular: *"Public places seem suitable for surveillance […] we don't feel that we are personally monitored"* (P1-II). Additionally, some participants also argued that they have no expectations of privacy in a public space: *"[…] in these places, privacy is out of the question"* (P7-II). Nevertheless, there was a minority of participants who did object to being monitored in public spaces: *"I would say that public spaces are public and therefore should not be monitored"* (P1-I). Lastly, surveillance was considered as unacceptable in private spaces such as one's home and in places *"where you live your private life"* (P1-II).

5.4 Surveillance laws and regulations

During the last part of the focus group sessions, issues relating to surveillance laws and regulations were discussed, including citizens' privacy rights, the effectiveness of surveillance laws and regulations and length of data storage.

5.4.1 Effectiveness of legislation

The first issue discussed was whether surveillance laws and regulations are effective in providing the necessary protection to citizens. Firstly, it should be pointed out that some participants emphasised their limited knowledge and awareness with respect to privacy laws and, thus, about their rights as citizens: "*I'm not very familiar with it [privacy legislation]"* (P3-I). In turn, this might have presented a difficulty for participants to determine whether the existing laws and regulations do indeed offer the required protection.

Participants expressed rather varied opinions about the perceived level of protection. Some participants clearly stated that they do not feel protected by current legislation, expressing discontent towards the state's protection of citizens' rights: *"Romanian law in this field is lacking, just like in other areas"* (P1-II). These participants see current legislation as inadequate and argued that legislation should be made stricter with the inclusion of more restrictive regulations.

On the other hand, others suggested that the problem does not lie with the legislation as such, which they perceived as offering adequate protection; these participants argued that the central issue is that the legislation is not abided by, here possibly also alluding to a lack of enforcement: *"Legislation exists but I don't think that it is implemented across all cases"* (P3-I). Other participants expressed their satisfaction with the level of protection currently offered by the legislation: *"I consider that they [privacy laws] are very good, and the more restrictive they are, the more protection they offer to [citizens'] private lives. They make me feel protected"* (P6-II).

5.4.2 Length of data storage and accessibility

The expectations of participants regarding the storage of their private data were rather varied. Whilst some participants claimed that storage period *"does not matter"* (P6-III), others declared that this made a difference to them, and proceeded to provide numerous time spans which they believed would be appropriate. Some participants argued for a time span which is "*as short as possible"* (P1-I), ranging from a few hours to a couple of months, while others claimed that a longer duration, ranging from six months to five years, would be more appropriate: *"It should be kept long enough to be used in the future"* (P3-II). Moreover, a minority of respondents appeared to argue for an indefinite storage period.

A couple of participants stated that the determination of an acceptable storage period would *"vary case by case"* (P2-III). Although these respondents did not discuss this in detail, they maintained that length

of storage should be contingent on a number of factors, including the type of data in question, the issue of who has access to the stored data, and, lastly, the purpose of use: *"I believe the collected information should be stored and used only for the purpose for which it was collected for and there should be strong laws to ensure this"* (P7-II).

6. Conclusion

Romanian participants had a relatively high awareness that citizens are subject to surveillance in the main spaces considered during the discussion. The results indicate 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 security-related purposes as well as for marketing purposes in commercial spaces. Although there was awareness of being under surveillance by different monitoring methods and technologies, it appears that some participants, particularly those belonging to Group 3 (45+ years), found it difficult to understand the exact nature of smart surveillance.

Whilst the majority of participants were principally against the massive integration of data mainly because it was perceived as a threat to citizens' privacy, it appears that attitudes in relation to the acceptance of surveillance – smart or non-smart – were rather polarised. A number of participants appeared to willingly accept a decrease in privacy for increased security while others actually questioned the notion of surveillance-based security. Additionally, perceiving surveillance as a means of control, a number of participants argued that what is at stake is not only citizen privacy, but individual freedom. It seems that at the heart of the matter, what seems to reassure some participants is not surveillance but rather the country's moral fibre: "*In Romania, it is rather our spirit, our education [that] makes me feel protected; our way of being"* (P2-I).

Some participants inevitably alluded to the pervasive dilemma in this field – that of striking a balance between liberty rights and national security:

> *"We live in a world where disorder and crime seem to be on the increase and I think it is necessary to have certain measures to diminish them and improve surveillance for the purpose of preventing potentially unwanted events. However, I believe that there must be a limit to everything; otherwise there is a risk we build a big-brother society where everything is controlled" (P7-II).*

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

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

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

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

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

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

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

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

- ☐ Yes
- ☐ No

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

- ☐ **Yes**
- ☐ **No**

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

- ☐ Yes
- ☐ No

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

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

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

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

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

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

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

discussion.	***Card 3 - Object and product detection devices**: Knife arches (portal) and X-ray devices* ***Running total: 40min***
Presentation of MIMSI scenario to participants **[30mins]** - *To explore participants' understanding of the implications of MIMSI* - *To explore participants' feelings, beliefs and attitudes vis-à-vis the sharing of personal information*	***Item 4*** *Present the following hypothetical scenario to the group. A recording of the phone conversation can be prepared beforehand and presented to the group.* ***Phone conversation with the Customer Care Agent at the main branch of the Public Employment Service*** ***Customer Care Agent**: Good morning this is Sharon speaking, how are you Mr. Brown? We were expecting your call after your work contract ended over a month ago.* ***Mr. Brown**: Erm...yes in fact that's why I'm calling...* ***Customer Care Agent**: Well, I'm actually not surprised you called now...how was your holiday in Cyprus? I am sure your wife and kids enjoyed the resort you were staying in...* ***Mr. Brown**: Yes it was a lovely holiday...and how do you know all this?* ***Customer Care Agent**: Well, it is in the system, Mr. Brown....obviously. Anyways, better get a head start on finding a new job...what with the cost of your family holiday and your car payment coming up soon...not to mention your VISA payment on the 22nd of this month...* ***Mr. Brown**: Is this also in your system?* ***Customer Care Agent**: Yes, of course Mr. Brown. By the way, good choice on the book you bought online...I read it myself and it gave me some really good tips...*

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

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

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

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

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

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

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

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

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

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

Aims
1. Participants' first reactions including:

Possibility / impossibility of scenario

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

Acceptability / unacceptability of scenario

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

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

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

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

affect their privacy

manner affect your privacy?

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

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

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

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

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

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

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

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

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

Running Total: 1 hour 15min

Reactions to scenarios

[About 20mins]

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

Item 5

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

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

whether these technologies effect privacy and hence revolve around the security - privacy trade-off

automatically should there be a cause for alarm and risk to any citizen.

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

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

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

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

Aims:

1. Security climate and level of threat

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

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

2. Deployment of specific technologies

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

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

3. Locations of deployment such as:
Airports
Malls

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

Streets *4. Existence of laws and other safeguards (in relation to the collection, storage and use of data)* *5. Length of storage of surveillance data*	***being monitored?*** ***4a. What do you think about privacy laws? Do they make you feel <u>protected</u>?*** ***4b. Are there any <u>safeguards</u> or conditions that you would find <u>reassuring</u>?*** ***5a. What do you think about the length of storage of surveillance data? Does it make a difference?*** ***To help you probe, provide the following examples to the participants:*** - ***Recordings of CCTV*** - ***The location and movement of cars*** - ***The storage of DNA, fingerprints and iris scans*** - ***The location of citizens who pose a risk to others*** - ***The location and movements of elderly people and children*** ***5b. If length of storage makes a difference, what would you consider as an <u>acceptable timeframe</u>?*** ***Running Total: 1 hour 35min***
Brief summary of discussion [5mins] ▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***Item 6 – Summing up session*** ***At the end of the focus group, it is helpful to provide a summary of the emerging points. Here you should aim at giving a brief summing up of the themes and issues raised during the discussion. After, you can ask for the following from the participants:*** - ***"How well does that capture what was said here today?"*** - ***"Is there anything we have missed?"*** - ***"Did we cover everything?"*** ***This brief session will give participants an additional opportunity to express their views and can also be used to elaborate on topics raised but not pursued at the time.*** ***Running Total: 1 hour 40 min***
Conclusion of focus group [5mins] ▪ ***Thank the participants*** ▪ ***Hand out the reimbursement*** ▪ ***Give information on SMART***	***Item 7 –Closure*** **With this last exercise our discussion has come to an end. May we take this opportunity to once again thank you for joining us and for sharing your opinions, experiences and thoughts.** ***At this point, hand out the reimbursements to the participants and inform the participants about the next steps.*** ***Give out more information about the SMART to the participants requesting such information.***

Total: 1 hour and 45 min

APPENDIX C – DISCUSSION GUIDELINES (ROMANIA)

Introducere	Informare
Primirea participanților - *Salutul participanților* - *Împărțirea etichetelor cu nume* - *Semnarea formularelor de consimțământ*	*Urați-le bun venit participanților de îndată ce sosesc. Oferiți-le un loc și eticheta cu numele.* *Distribuiți formularele de consimțământ participanților și rugați-i să le citească și să le semneze înainte de a începe interviul de grup. Acest lucru este important pentru a vă asigura că participanții înțeleg ce anume au fost de acord să facă.*
Introducere [aproximativ 10 min] - *Mulțumiri* - *Prezentarea echipei de facilitatori* - *Scopul* - *Confidențialitate* - *Durata* - *Reguli de bază pentru grup* - *Scurtă prezentare a fiecărui participant*	**Bine ați venit la acest interviu de grup și vă mulțumim pentru că ați fost de acord să participați la această întâlnire. Apreciem faptul că ne-ați oferit acest timp din programul dumneavoastră încărcat ca să participați la acest proiect și participarea dumneavoastră este foarte apreciată.** **Numele meu este _____ și voi conduce discuțiile în cadrul grupului. Voi fi asistat de către _____ co-moderatorul meu, care va lua notițe și va înregistra discuția noastră.** *Prezentați alți colegi care mai sunt prezenți* **Întâlnirea noastră va dura între o ora și jumătate și două ore, și pentru că vom înregistra această discuție, vă rugăm să vorbiți clar; părerile și gândurile dumneavoastră sunt foarte importante pentru această cercetare, și nu dorim să ratăm vreunul din comentariile dumneavoastră.** **După cum am menționat mai devreme, atunci când ați fost contactați ca să participați la această discuție, tema acestei întâlniri este Tehnologie și Confidențialitate, și este organizată ca parte a proiectului SMART, co-finanțat de Comisia Europeană. Cei care doresc să afle mai multe despre acest proiect SMART, vă rugăm să ne spuneți și vă vom da mai multe informații la finalul acestei întâlniri.** *În acest moment este important să nu divulgați alte detalii despre conținutul discuțiilor, pentru a nu influența ceea ce se va discuta.* **După cum v-am informat când ați citi și semnat formularul de consimțământ, tot ce se va înregistra în timpul întâlnirii va fi confidențial și identitatea dumneavoastră va rămâne anonimă. Aceasta înseamnă că toate comentariile dumneavoastră vor fi folosite doar de cei implicați în acest studiu și în publicații științifice referitoare la acest studiu, și vor deveni anonime înainte de a fi raportate. Prin urmare, informațiile pe care le vom include în raport nu vă vor identifica în nici un fel ca participant. În acest sens, fiecare veți primi un număr, iar acest număr va fi folosit în raport.** **De asemenea doresc să mă asigur că toți participanții se simt suficient de confortabil ca să-și împărtășească părerile. Pentru a face posibil acest lucru, vă prezint următoarele reguli de bază:** ▪ **Dorim să auzim fiecare persoană din grup – ne interesează părerea tuturor** ▪ **Nu există răspunsuri corecte sau greșite, așadar să ne respectăm opiniile unii altora** ▪ **Vă rugăm să vă asigurați că telefoanele dvs. mobile sunt setate pe modul silențios, astfel încât discuția să nu fie întreruptă** ▪ **Este important să faceți comentariile fiecare pe rând, deoarece**

	opinia fiecărui participant este importantă. Să fim de acord așadar să nu vorbim deodată, altfel va fi dificil să înregistrăm tot ce se spune în timpul discuției ▪ **Să ne punem de acord să respectăm confidențialitatea unul altuia, astfel încât toată lumea să se simtă confortabil vorbind deschis.** **Dacă dorește cineva să propună și alte reguli de bază, simțiți-vă liberi să faceți grupului sugestiile dumneavoastră.** **Are cineva întrebări înainte de a începe?** **Bine, dați-mi voie să încep prin a vă ruga să vă prezentați pe scurt grupului, fără a oferi informații personale. Vă rog să ne spuneți pe rând numele dumneavoastră și poate ceva despre dumneavoastră. Voi începe eu... *(faceți o scurtă prezentare despre dumneavoastră)*** *Timp de lucru: 10 min*
Obiective	**Puncte de discuție și exerciții**
Exercițiu de asociere de cuvinte **[Aproximativ 5min]** - *Joc de asociere de cuvinte, pentru a sparge gheața* - *Stabiliți principalele asocieri mentale cu temele cheie* - *Începeți discuția de grup*	***Punctul 1*** **Pentru inceput, vom juca un joc scurt: voi citi un cuvant si as vrea sa spuneti primele doua lucruri care va vin in minte cand auziti cuvantul. Sa incercam intai un exemplu: Care este primul lucru care va vine in minte daca spun cuvantul "*mancare*"? Este de preferat sa incercati sa va ganditi doar la cuvinte sau expresii scurte, evitand descrierile lungi.** *Citeste (cate unul pe rand):* *Tehnologie, confidentialitate, securitate nationala, informatii personale, siguranta personala* *Timp de lucru: 15min*
Discuție despre experiențele de zi cu zi legate de supraveghere **[20min]** - *Pentru a explora experiența participanților referitoare la supraveghere și cum o percep aceștia* - *Pentru a explora conștientizarea participanților și cunoștințele acestora despre diferite tipuri de tehnologii de supraveghere*	***Punctul 2*** **Sa vorbim despre altceva. Vreau sa va ganditi la momente in care simtiti ca fie dumneavoastra, fie actiunile dumneavoastra sunt observate, precum si orice momente in care sunteti constienti ca se colecteaza informatii despre dumneavoastra. Sa incepem prin a ne gandi la activitati pe care le faceti de obicei in viata de zi cu zi. Sa luam urmatoarele situatii ca exemple.** **Scenariul 1: Supermarket** **Ca un prim exemplu, putem considera o iesire la cumparaturi al magazinul la care mergeti de obicei. Va puteti impartasi gandurile despre acest lucru??** **Scenariul 2: Calatoriile** **Sa mergem mai departe catre o alta situatie, de data aceasta legata de calatorii. Ce ziceti despre calatoriile cu avionul?** **Scenariul 3: Locul public (e.g. muzeu, stadion)** **Imaginati-va acum ca vizitati un loc public, precum un muzeu sau ca participati la un eveniment sportiv precum un meci sau la un concert. Ce**

	fel de activitati credeti ca ar fi inregistrate? **Scenariul 4: Dispozitive mobile** **Sa vorbim despre un ultim exemplu. Ganditi-va la momentele cand folositi telefonul mobil. Ce credeti ca se inregistreaza in acest caz?**
Scopuri: *1. Explorarea conștientizării participanților și cunoștințele despre tehnologii* *2. Explorarea experienței participanților de a fi monitorizați în diferite roluri,* *3. Explorarea înțelegerii participanților asupra destinației finale a informațiilor lor* *4. Explorarea părerilor participanților despre motivul pentru care acțiunile și comportamentele lor sunt observate, monitorizate, și colectate*	*Pentru fiecare punct, si acolo unde este relevant, examinati in detaliu urmatoarele:* ***1. Cum este colectata informatia:*** ***a. Ce tipuri de tehnologie credeti ca se foloseste pentru colectarea informatiilor personale despre dumneavoastra?*** ***2. Ce tip de informatii se colecteaza:*** ***b. Ce tip de informatii personale credeti ca se colecteaza?*** ***3. Cine colecteaza informatiile:*** ***a. Cine credeti ca este responsabil de colectarea si inregistrarea informatiilor personale ale dumneavoastra?*** ***b. Unde credeti ca vor ajunge informatiile personale ale dumneavoastra?*** ***4. De ce se inregistreaza, se colecteaza si se stocheaza informatiile:*** ***a. De ce credeti ca se inregistreaza si se colecteaza informatiile personale ale dumneavoastra?*** ***b. In ce moduri credeti ca vor fi utilizate informatiile personale?*** *Timp de lucru: 35min*
Prezentarea cartonașelor cu diferite tehnologii și aplicații [10min] *Expunerea*	***Punctul 3*** *Prezentati grupului urmatoarele trei cartonase (fiecare reprezentand un grup de diferite tehnologii si aplicatii). Cartonasele vor include urmatoarele descrieri:* ***Cartonasul 1 – Tehnologii de recunoastere & urmarire a persoanelor sau***

participanților la o selecție de tehnologii și aplicații SMART relevante, pentru a asigura o mai bună înțelegere și astfel pentru a facilita discuția.	***evenimentelor**: Miscare automata a camerelor TV cu circuit inchis (CCTV); Cititor automat de placute de inmatriculare (ANPR) sau identificare automata a numarului vehiculului (AVNI); si dispozitive de urmarire precum urmarirea telefonului mobil si identificare prin frecventa radio (RFID)* ***Cartonasul 2 – Date biometrice**: Tehnologiile biometrice includ scanarea amprentelor si a irisului; si recunoastere faciala automata (AFR)* ***Cartonasul 3 – Dispozitive de detectare a obiectelor si produselor**: porți de detectare a metalelor (portal) si dispozitive cu raze X* *Timp de lucru: 40min*

Prezentarea scenariului MIMSI (intrări multisenzor integrate masiv) participanților

[30min]

- *Explorarea înțelegerii participanților referitoare la implicațiile MIMSI*

- *Explorarea sentimentelor, părerilor și atitudinilor participanților cu privire la împărtășirea informațiilor personale*

Scopuri

Punctul 4

Prezentati grupului urmatorul scenariu ipotetic. Se poate pregati dinainte o inregistrare a unei convorbiri telefonice care sa fie prezentata grupului.

Convorbire telefonica cu Agentul de Relatii cu Clientii la sucursala principala a unui Serviciu Public de Ocupare a fortei de munca.

***Agent relatii cu clientii**: Buna dimineata, numele meu este Maria, ce mai faceti domnule Pop? Asteptam telefonul dumneavoastra, in urma incetarii contractului dumneavoastra de munca acum mai bine de o luna.*
***Dl. Pop**: Hmm...da, de fapt de aceea va sun...*
***Agent relatii cu clientii**: Pai, de fapt nu sunt surprinsa ca ati sunat acum... cum a fost vacanta dumneavoastra in Cipru? Sunt sigura ca sotiei si copiilor le-a placut statiunea unde ati stat...*
***Dl. Pop**: Da a fost o vacanta minunata... si cum stiti dumneavoastra toate aceste lucruri?*
***Agent relatii cu clientii**: Pai, este in sistem, domnule Pop....evident. Oricum, e mai bine sa aveti un avantaj in gasirea unui nou loc de munca...cu costurile vacantei cu familia si plata masinii care urmeaza in curand... ca sa nu mai spun de plata VISA pe data de 22 a lunii curente...*
***Dl. Pop**: Si aceste lucruri sunt in sistemul dumneavoastra?*
***Agent relatii cu clientii**: Da, desigur domnule Pop. Apropo, cartea pe care ati cumparat-o online este o alegere buna... O citesc si eu si mi-a dat niste sfaturi foarte bune...*
***Dl. Pop**: Hmmm...bine...referitor la serviciul acesta de gasire a unui nou loc de munca, trebuie sa va ofer o fotografie a mea mai recenta?*
***Agent relatii cu clientii**: Nu domnule Pop, deja am avut grija de asta, desigur! Avem multe fotografii recente in sistemul nostru. Ceea ca mi-a reamintit de ceva...v-ati bronzat frumos in vacanta! Trebuie sa fi fost vreme frumoasa! Inainte de a uita, referitor la fotografie, preferati una in care purtati ochelari sau fara?*
***Dl. Pop**: Oh...pai....fara este bine...deci referitor de inregistrarea mea, putem stabili o intalnire pentru candva saptamana viitoare?*
***Agent relatii cu clientii**: Dati-mi voie sa verific in sistem...ce ziceti de miercuri la amiaza? Oh asteptati o secunda! Tocmai am observat ca aveti programare la medic exact atunci. Si sunt sigura ca nu vreti sa o ratati, de vreme ce nivelul de colesterol este cu siguranta important! Ce spuneti de joi dimineata la prima ora, la 9?*
***Dl. Pop**: Joi dimineata va fi bine...trebuie sa aduc vreun document cu mine?*
***Agent relatii cu clientii**: Nu domnule Pop, avem deja in sistem toate informatiile de care avem nevoie.*
***Dl. Pop**: Sunt sigur...*
***Agent relatii cu clientii**: Va multumim ca ati sunat domnule Brown si ne vom vedea saptamana viitoare. Apropo, savurati-va ceasca de cappuccino la Cafe Ole'...*
***Dl. Pop**: Asta fac...la revedere...*
...

Dupa prezentarea scenariului precedent grupului, examinati in detaliu urmatoarele:

1. Prima reacție a participanților, inclusiv:

Posibilitatea / imposibilitatea realizării scenariului

Acceptabilitatea / inacceptabilitatea scenariului

2. Părerile și atitudinile participanților despre cum le afectează tehnologia sau cum le-ar putea afecta intimitatea

3. Părerile și atitudinile participanților cu privire la tipuri de informații precum: Înregistrări medicale; Informații financiare; Fotografii și localizare.

4. Părerile și atitudinile participanților cu privire la colectarea și partajarea informațiilor personale către terți.

5. Părerile și atitudinile participanților cu privire la beneficiile și dezavantajele monitorizării

1a. Cum v-ati simti daca vi s-ar intampla acest lucru dumneavoastra?
(De asemenea, examinati in vederea stabilirii gradului de control /neputintei simtite de participanti intr-un scenariu ipotetic precum acesta)

1b. Cum ati reactiona daca vi s-ar intampla dumneavoastra acest lucru? Ce ati face?

1c. Este un astfel de scenariu posibil / imposibil?
1d. Este un astfel de scenariu acceptabil / inacceptabil?

2a. In ce masura credeti ca aplicatiile "stand alone" (tehnologii individuale) va afecteaza intimitatea?

2b. In ce masura credeti ca "tehnologiile smart" adica acelea care proceseaza datele in mod automat (sau semi-automat) va afecteaza intimitatea?

3a. Ce tip de informatii personale considerati ca sunt acceptabile spre a fi colectate, utilizate si / sau partajate?

3b. Impotriva carui tip de informatii personale ati obiecta la colectare, utilizare si / sau partajare?

4a. Ce credeti despre colectarea, utilizarea si partajarea informatiilor personale ale dumneavoastra, de catre stat?

4b. Ce credeti despre colectarea, utilizarea si partajarea informatiilor personale ale dumneavoastra, de catre entitati private (precum cele comerciale)?

5a. Credeti ca exista vreun beneficiu in monitorizarea actiunilor si comportamentului dumneavoastra?

5b. Credeti ca exista vreun inconvenient in monitorizarea actiunilor si comportamentului dumneavoastra?

Timp de lucru: 1 ora 15min

Reacții la scenarii

[Aproximativ 20min]

- *Stimularea unei dezbateri pentru a explora percepțiile participanților despre "compromisul securitate contra intimitate".*
- *Aici, în discuție nu are trebui să se ia în considerare dacă aceste tehnologii vor crește sau nu securitatea – aceasta are trebui luată ca atare. Discuția ar trebui centrată în principal pe posibilitatea ca aceste tehnologii să afecteze intimitatea și astfel preocuparea să fie asupra compromisului securitate contra intimitate*

Scopuri:

1. Climat de siguranță și nivelul pericolului

2. Desfășurarea tehnologiilor specifice

Punctul 5

Pe parcursul urmatorului exercitiu vom discuta urmatorul scenariu ipotetic. Imaginati-va urmatorul scenariu:

Datorita unei cresteri semnificative a *criminalitatii violente* in capitala, inclusiv *o multime de rapiri si omoruri care par la intamplare si fara legatura*, statul a decis introducerea supravegherii CCTV in toate spatiile publice, atat proprietatile publice (precum pasajele subterane, gradinile publice si toalete publice) precum si cele private (precum magazine, mall-uri si taxi-uri) care vor permite recunoasterea faciala automata. In plus, tuturor masinilor care trec prin principalele puncte de control li se va inregistra numarul de inmatriculare. Exista de asemenea planuri de a instala senzori in toate zonele publice care pot detecta zgomote puternice ca de exemplu strigatul cuiva. Se va solicita pentru toti cetatenii colectarea amprentelor si ADN-ului precum si scanarea irisului. Statul a decis de asemenea ca toti cetatenii care au fost identificati ca fiind un posibil risc pentru altii vor fi etichetati electronic pentru a monitoriza si urmari miscarile lor. Pentru siguranta lor, persoanele in varsta si copiii cu varsta pana la 12 ani vor fi de asemenea etichetati electronic. Toate datele din aceste tehnologii diferite vor fi stocate in baze de date asociate si administrate de catre organele de politie, care vor fi notificate automat in cazul unei alarme si a riscului pentru orice cetatean.

Spuneti-le participantilor sa isi imagineze scenariul de mai sus oricum cu urmatoarele variatii:

Variatia 1: Desi are loc o crestere semnificativa a criminalitatii violente in majoritatea oraselor invecinate, in orasul in care locuiti dumneavoastra nu are loc nici o crestere a acesteia. Totusi statul decide sa introduca masuri de supraveghere, ca masura de precautie.

Variatia 2: In intreaga tara are o rata a criminalitatii foarte redusa in general, dar statul totusi decide sa introduca masuri de supraveghere ca precautie dupa ce intr-un oras invecinat a avut loc un incident izolat in timpul caruia un numar de oameni au fost impuscati si grav raniti de un barbat care a deschis focul intr-un mall.

In timpul discutiilor asupra scenariului de mai sus / variatiilor, examinati in detaliu urmatorii factori si cum ar putea sa afecteze "compromisul securitate contra intimitate":

1a. Ce anume va face sa va simtiti in siguranta in scenariul prezentat?

1b. Ce anume va face sa va simtiti vulnerabil in scenariul prezentat?

1c. Ati fi dispus sa va sacrificati intimitatea daca gradul de pericol ar fi diferit in functie de variatia 1 si 2 a scenariului?

2. Dintre tehnologiile smart descrise in scenariu, adica

CCTV cu recunoastere faciala automata,
Recunoastere automata placute de inmatriculare (ANPR),
Senzori (cu capacitatea de a detecta zgomote puternice),
Tehnologii biometrice (inclusiv amprentarea) si
Etichetarea electronica (care utilizeaza identificarea prin frecventa radio RFID)

2a. Pe care dintre tehnologii le considerati <u>acceptabile</u>? De ce?
2b. Care dintre tehnologii considerati ca <u>invadeaza</u> si ameninta intimitatea dumneavoastra? De ce?
2c. Ce credeti despre aceste tehnologii automate (sau semi-automate) in care decizia finala este luata de sistem si nu de un operator uman?

3. Locațiile de desfășurare, precum:
Aeroporturi
Mall-uri
Străzi

3a. Care dintre locatii le considerati <u>acceptabile</u> in vederea monitorizarii? De ce?
3b. Care dintre locatii le considerati <u>inacceptabile</u> in vederea monitorizarii?

4. Existența legilor și a altor măsuri de protecție (cu privire la colectarea, stocarea și utilizarea datelor)

4a. Ce parere aveti despre legislatie cu privire la intimitate? Va fac sa va simtiti <u>protejat</u>?

4b. Exista <u>masuri de protectie</u> sau conditii pe care le considerati <u>linistitoare</u>?

5. Durata stocării datelor de supraveghere

5a. Ce credeti despre durata stocarii datelor de supraveghere? Conteaza acest lucru?
Pentru a va ajuta sa stabiliti, dati participantilor urmatoarele exemple:
- ***Inregistrarile CCTV***
- ***Locatia si miscarea masinilor***
- ***Stocarea ADN-ului, amprentelor si scanarilor irisului***
- ***Locatia cetatenilor care reprezinta un risc pentru altii***
- ***Locatia si miscarea persoanelor in varsta si a copiilor***

5b. Daca durata stocarii conteaza, cat considerati ca ar fi <u>durata acceptabila</u>?

Timp de lucru: 1 ora 35min

Obiective	Sesiune de recapitulare
Scurt rezumat al discuției [5min] ▪ *Confirmați principalele puncte discutate* ▪ *Oferiți ocazia de a detalia ceea ce s-a spus*	***Punctul 6*** ***La finalul intalnirii, este util sa oferiti un rezumat al problemelor dezvoltate. Aici ar trebui sa aveti ca scop prezentarea unui rezumat scurt al temelor si problemelor discutate in timpul intalnirii. Dupa aceea, puteti adresa participantilor urmatoarele intrebari:*** - **"Cat de bine include acest lucru ceea ce s-a discutat azi aici?"** - **"Am uitat sa mentionam ceva?"** - **"Am cuprins totul?"** ***Aceasta sesiune scurta va oferi participantilor o posibilitate in plus de a-si exprima parerile si poate fi folosita de asemenea pentru detalierea problemelor ridicate dar nediscutate in acel moment.***

Timp de lucru: 1 ora 40 min

Obiective	Încheiere
Concluzia interviului de grup [5min] ▪ ***Mulțumiri participanților*** ▪ ***Efectuați rambursarea*** ▪ ***Oferiți informații despre SMART***	***Punctul 7*** **Prin acest ultim exercitiu, discutia noastra a ajuns la final. Sa folosim aceasta oportunitate pentru a va multumi din nou ca ne-ati fost alaturi si ne-ati impartasit parerile, experientele si gandurile dumneavoastra.** ***In acest moment, efectuati rambursarea participantilor si informati-i despre pasii urmatori.*** ***Oferiti-le participantilor interesati mai multe informatii despre SMART.*** ***Total: 1 ora 45 min***

APPENDIX D – DEBRIEFING FORM

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

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

APPENDIX E – CONSENT FORM

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

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

1.1. Commercial space

1.1.1. Awareness of different surveillance methods/technologies

1.1.1.1. CCTV

1.1.1.2. Loyalty cards

1.1.1.3. Financial monitoring

1.1.1.4. Theft detection devices

1.1.2. Perceived purposes

1.1.2.1. Security purposes

1.1.2.2. Monitoring of employees

1.1.2.3. Consumer behaviour research (for advertising and marketing purposes)

1.2. Boundary (border) space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. CCTV

1.2.1.2. Smart CCTV with AFR

1.2.1.3. Biometric technologies

1.2.1.3.1. Fingerprinting

1.2.1.3.2. Retinal scanning

1.2.1.3.3. Iris scanning

1.2.1.4. Object and product detection devices

1.2.1.4.1. Luggage controls

1.2.1.4.2. Body scanners

1.2.1.4.3. Metal detectors

1.2.1.5. Monitoring of personal data

1.2.1.5.1. Passport control

1.2.1.5.2. Passenger lists

1.2.1.5.3. Airline booking system

1.2.2. Perceived purposes

1.2.2.1. National security

1.2.2.2. Traveller safety

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV

1.3.1.2. Smart CCTV with AFR

1.3.1.3. Object detection devices

1.3.1.4. Microphones

1.3.1.5. Collection of personal data

1.3.2. Perceived purposes
1.3.2.1. Visitor safety
1.3.2.2. Protection of property
1.3.2.3. Prevention and detection of crime
1.3.2.4. Crowd monitoring and regulation of visitor flow

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. Recording of conversations (wiretapping)
1.4.1.3. Location tracking via GPS
1.4.1.4. Collection of data through smart phone applications
1.4.2. Perceived purposes
1.4.2.1. Marketing and financial purposes
1.4.2.2. Crime prevention, detection and prosecution

2. Perceptions and attitudes towards smart surveillance and dataveillance
2.1. Feelings
2.1.1. Extreme discomfort
2.1.1.1. Shock
2.1.1.2. Vulnerability
2.1.1.3. Helplessness and resignation
2.1.2. Anger and indignation

2.2. Behavioural intentions
2.2.1. Passive reactions
2.2.1.1. Immediate withdrawal
2.2.1.2. No action taken
2.2.2. Self-protection strategies
2.2.2.1. Investigate
2.2.3. Take legal action

2.3. Beliefs
2.3.1. Likelihood of smart surveillance and dataveillance
2.3.1.1. Technical aspect
2.3.1.1.1. Possible due to integration of data
2.3.1.1.2. Self-responsibility
2.3.1.2. Legal aspect
2.3.1.2.1. Legal restrictions
2.3.1.3. Ethical aspect

2.3.1.3.1. Invasion of privacy

2.3.2. Acceptance of dataveillance

2.3.2.1. Consent

2.3.2.2. Access to data

2.3.2.2.1. State

2.3.2.2.2. Private entities

2.3.2.3. Type of data stored and shared

2.3.3. Perceived effectiveness of smart technologies

2.3.3.1. Decision-making capabilities of automated systems

2.3.3.2. Human agency

2.3.3.3. Efficiency of smart technologies in investigation of crime

3. Security-privacy trade-offs

3.1. Acceptance of technological surveillance

3.1.1. Feelings

3.1.1.1. Safety

3.1.1.2. Vulnerability

3.1.2. General beliefs

3.1.2.1. Safety and peace of mind: the "caring" function of surveillance

3.1.2.2. Extreme form of control: association with a police state

3.1.2.3. Observation of citizens: criminalisation of citizens

3.1.2.4. Violation of privacy and freedom

3.1.3. Effectiveness of surveillance

3.1.3.1. Increased personal safety and public security

3.1.3.2. Ineffectiveness in offering protection

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

3.2. Perceptions of different technologies

3.2.1. CCTV

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

3.2.2.2. Sense of discomfort and uneasiness

3.2.2.3. Treat to freedom

3.3. Locations of deployment

3.3.1. Acceptable: the 'caring function' of surveillance

3.3.1.1. Public places

3.3.1.2. High risk areas

3.3.2. Unacceptable

3.3.2.1. Private spaces and private spheres

4. Surveillance laws and regulations

4.1. Feelings and beliefs

4.1.1. Knowledge and awareness of legislation

4.1.2. Effectiveness of laws and regulations

4.1.3. Length of data storage and accessibility