Beliefs and attitudes of citizens in the Czech Republic towards smart surveillance and privacy

Noellie Brockdorff[1], Sandra Appleby-Arnold[1], Christine Garzia[1], M Myska[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic

April 2014

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

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

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

Table of Contents

1. Key Findings

This document presents the Czech Republic results of a qualitative study undertaken as part of the SMART project – "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727). The analysis and results are based on a set of three focus group discussions comprising of 28 participants, which were held in order to examine the beliefs and attitudes of citizens towards smart surveillance and privacy.

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

The Czech participants revealed a general awareness that, as citizens, they are subjected to surveillance in different contexts. Overall, it appears that surveillance in commercial, boundary and public spaces has undergone a process of acceptance, with participants recognizing the various uses of surveillance in these spaces including the monitoring of customer behaviour and surveillance for security functions. On the other hand, participants revealed the most ambivalent feelings and beliefs in relation to the technological surveillance of mobile phone data, where their extensive technological knowledge gave rise to feelings of insecurity and lack of control in all age groups.

In order to gauge participants' attitudes and beliefs on the massive integration of data, the groups were presented with a fictional scenario illustrating the occurrence of complex surveillance. After an initial intense reaction to this situation, the participants proceeded to differentiate between technical, legal and ethical aspects. Despite the considered likelihood of such scenario, from a technical perspective the majority of participants in all age groups perceived most surveillance as currently still based on stand-alone technologies. However, their predominant belief was that such occurrence would mainly depend upon individual and institutional ethics. To a much lesser extent, some participants argued that existing laws would prohibit such intrusive surveillance from happening.

With regards to the conceptualisation, and understanding, of technological surveillance, it appears that most participants had difficulty in understanding the exact nature of smart surveillance. In particular, when referring to smart technologies they mostly imagined CCTV with automated face recognition (AFR), occasionally linked with voice and gait recognition. When comparing the effectiveness of traditional technologies and smart technologies, most participants focusing on the difference between automated and non-automated systems, equating non-automated technologies with traditional methods and automated with smart technologies. Ambivalent attitudes were expressed in this regard;

while on one hand, the use of automatised systems was perceived as resulting in a more objective and impartial decision-making process, on the other hand the majority of participants revealed feelings of discomfort since they feared that the use of smart technologies carries the risk of systematic misjudgment. In view of this, most participants argued that there should always be a human operator in the surveillance process who makes the final evaluation.

In relation to the general acceptance of technological surveillance, it appears that this was strongly contingent on the location of, and motivation for surveillance. Generally, though, surveillance was not perceived as increasing feelings of safety. On the contrary, systematic and comprehensive smart surveillance was perceived as unacceptable, categorising each individual citizen as a potential risk. Different technologies and methods also appeared to meet different levels of acceptance: while CCTV, sound detectors and automated license plate recognition (ALPR) seemed to be widely accepted as some form of impersonal or invisible surveillance, the use of biometric surveillance revealed a strong discomfort amongst the participants in all age groups. Similarly, the use of electronic tagging and GPS surveillance was perceived not only as violating privacy but also as restricting citizens' freedom.

Regarding the effectiveness of surveillance laws and regulations, feelings and beliefs varied considerably according to age; younger participants revealing a certain trust in the legal system, whilst older participants not feeling assured by the law. In this context, participants also discussed the accessibility of surveillance data and information sharing between public and private entities, with participants drawing a clear distinction between publicly and privately gathered surveillance data. Here, the general risk of data misuse was considered to be greater within private companies, but data sharing practices of public authorities were perceived as carrying the greater risk to the citizen. Overall, the secrecy surrounding the sharing of surveillance data between private and public entities appeared to raise insecurity amongst all participants.

It appeared that it is generally accepted that the control and power balance in the use of traditional surveillance technologies is an illusion. However, there also appeared some indication that concepts of smart surveillance may be perceived as still being under democratic negotiation between the state and its citizens, with both parties sharing the duty of keeping control.

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 the Czech Republic is Masarykova Univerzita (MU).

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

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

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

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

3. Methodology

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

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

3.1 Recruitment process

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

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

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

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

3.2 Discussion guidelines

Discussion guidelines (see Appendix B) were developed with the aim of gauging citizens' awareness and understanding of smart surveillance technologies and also at gaining an in-depth understanding of citizens' beliefs and attitudes towards smart surveillance and privacy. The discussion guidelines were developed and further refined following a pilot study conducted in November 2012. The discussion

guidelines were designed to tackle the main themes under study through a variety of scenarios. While some scenarios dealt with surveillance in everyday contexts likely to be encountered by research participants, other scenarios were hypothetical in nature and their aim was to elicit the feelings, beliefs and attitudes of the participants in relation to dataveillance, the massive integration of data from different 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 Czech version of the discussion guidelines can be found in Appendix C.

3.3 Focus group procedure

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

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

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

3.4 Data analysis

After conducting the focus groups, all sessions were fully transcribed in the local language and subsequently translated into English. The de-briefing forms were also translated into English. The coding process was carried out by three researchers and was based on 3 different data sets (the English transcripts from Austria, Czech Republic and Italy). An initial coding structure was developed through

the process of coding and re-coding as the transcripts were read and interpreted. Such a process initialised a critical recategorising and rethinking of the codes first applied, and allowed for a more focused data analysis and drawing together of overarching themes. Thus, the initial coding map was modified as the analysis unfolded. This process of revision was concluded once no new themes emerged and a final coding map was agreed upon. Nevertheless, the emergence of additional lower order codes was not excluded since the analysis of the remaining transcripts was still pending at this stage. The coding map for this report can be found in Appendix F.

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

4. Description of the Sample

The data analysis for the Czech Republic is based on 28 participants and the composition of the three groups is depicted in the following table:

Participant number	Group 1 – 18-24 years	Group 2 – 25-44 years	Group 3 – 45+ years
P1	F	M	F
P2	M	M	F
P3	F	F	F
P4	M	F	M
P5	M	M	M
P6	F	M	M
P7	F	F	M
P8	F	M	F
P9	F	F	F
P10	M	_	_
Total	**10**	**9**	**9**

The atmosphere in Group 1 (18-24 years) was described as rather tense at the beginning; nevertheless, although the participants were not very talkative at the start, they clearly made an effort to be more actively involved as the discussion progressed. The participants who were considered as less talkative also contributed, albeit later on. In spite of the awkward start, overall it appears that the discussion flowed well in this Group.

With regards to Group 2 (25-44 years), the atmosphere was described by the moderators as being more formal then the other two groups. In addition, it appears that the group dynamics were poor and that the discussion was rather forced. In particular, two participants (P8 and P9) were especially passive. On the other hand, it seems that two other participants (P4 and P6) tried to compensate for the lack of participation of the rest of the group, with the result that they contributed substantially to the discussion.

The atmosphere in Group 3 (45+ years) was considered as informal and rather relaxed, and the participants were described as friendly and cooperative. The discussion was generally smooth and free-flowing, so much so that at times the debate tended to stray from the topics under investigation. This was partly due to the older age of the participants; sometimes it proved difficult for the moderator (who was much younger than the participants) to properly manage the discussion since he did not want to give the impression of being disrespectful.

5. Results

5.1 Surveillance Technologies in Different Spaces

In order to establish what the focus group participants knew about different surveillance methods and 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 simply using their mobile phone, and the type of surveillance that could be taking place.

5.1.1 Commercial Space

In supermarkets, all respondents outlined CCTV as the predominant surveillance method. They perceived this technology as a shop owner's right within commercial premises; the data collected through CCTV they felt to be anonymous or "impersonal" information. At the same time, it appeared that they had become used to being "watched" by surveillance cameras for security reasons[2]. The protection of goods was described by some participants as not being surveillance as such – *"unless I give some data to the supermarket I don't feel under surveillance in any way"* (P2-III). On the other hand, use of CCTV footage of customer behaviour for market research was perceived as surveillance by some participants and appeared to raise more ambivalent feelings.

However, surveillance of customer behaviour via CCTV seemed still to be more accepted than through loyalty cards, potential reasons being that:

(1) the information collected via CCTV was perceived as being anonymous (see above), whereas data collected through loyalty card schemes could be linked back to a customer's name, address etc.;
(2) CCTV information was perceived to be used predominantly for general market research (e.g. shopping patterns) and have no impact on individual customers, whereas the use of loyalty card date was seen to result in the receiving of unwanted advertising;
(3) CCTV footage was perceived as somewhat more "controllable" through changing individual behavior (e.g., by looking away, behaving properly, etc. when in the presence of CCTV), whereas loyalty card schemes appeared to cause discomfort due to the uncertainty what specific data would actually be used, or even shared or sold to third parties.

Ultimately, it seemed that CCTV in commercial spaces had gone through a process of consumers' increasing acceptance: Respondents revealed a certain expectation that cameras should be placed in a way *"that the customer feels better and not under surveillance"* (P9-I), pointing additionally at a combination of denial and after-the-fact acceptance, which can be seen as a consequence of the simultaneous visibility and invisibility of technological surveillance.

[2] Prevention and detection of theft, but also safeguarding payment procedures.

The third surveillance method (apart from CCTV and loyalty card schemes) mentioned by a number of respondents was financial monitoring, i.e. the surveillance of debit or credit card movements. Here, it appeared that the respondents had a rather vague idea of the purpose of such surveillance. Rather than the monitoring of suspicious, i.e. fraud-related, financial transactions, participants expressed their suspicion that banks would also use debit/credit card information for marketing purposes. For example, by sharing such information with third parties – a perception which may be linked to the increasing number of large companies offering in cooperation with banks "free" credit cards which are also used as loyalty cards. Whereas such "blurring" may raise the discomfort of some, it may also be questioned to what extent consumers are actually able to disentangle the different functions and consequences.

5.1.2 Boundary Space

In the context of border control, i.e. in an airport which represents a kind of "boundary space", focus group participants appeared to know about a larger range of surveillance methods and technologies: CCTV, biometric surveillance, the monitoring of personal data via passport control or passenger lists, and x-ray as well as metal detectors. At the same time, it appeared that, contrary to what was the case in supermarkets, in border control the participants did imagine certain forms of smart surveillance taking place. Although not directly naming it as such, in their descriptions participants combined technologies, e.g. the surveillance of biometric information from passports with biometric information from body scanners, personal information from booking systems and bank/payment data, or they linked CCTV with automatic face recognition (AFR) systems.

However, it also appeared that participants were unsure about the existence of what they were describing. They seemed to feel slightly embarrassed to express their ideas given that they were suspicious, but rather uncertain, whether such surveillance systems really existed: *"I think there are systems for facial recognition, so even the cameras at the airport may surveil people and try to compare faces. But maybe I watch too many spy movies"* (P4-II).

The main purpose for use of surveillance in this space mentioned by participants, and accepted, was national security – in particular the fighting of terrorism and crime. In this boundary space, it appeared that they felt little concerned about being under surveillance themselves by a variety of private and public entities, and potentially different national authorities. Whereas the respondents did express their discomfort about a "mix-up" of private-commercial and public-state surveillance, their criticism rather targeted commercial surveillance conducted by private companies in public space, or using "public" surveillance data for private commercial purposes.

5.1.3 Common Public Spaces

Participants were strongly of the opinion that surveillance based on smart[3] technologies, in particular CCTV with automated face recognition (AFR), takes place in common public spaces such as museums, or mass events such as concerts or football matches. And that the collected data would then be checked against databases such as criminal records and/or ID card-related personal data with the purpose of identifying troublemakers or offenders. Generally, the participants revealed a belief that, particularly in mass events, smart surveillance provides safety and may even prevent crime – although the perceived main purpose of such technologies was the timely detection, limitation and prosecution of crime.

However, some respondents also expressed a view that such surveillance systems would, as a "side effect", record indiscriminately everything and everyone: *"There would be these cameras again, which will be pre-set and look only for certain people who disrupt order there – only that they record other people as well. I think that gives a lot of power to the security forces"* (P5-II). Mostly, though, this awareness did not appear to cause major concern. Rather it seemed to be linked to a form of acceptance which may represent an underlying desire to be looked after – the comforting feeling to be part of something which, perhaps, is reinforced by and merges with general feelings of belonging in mass events where shared interests are celebrated (sports, music, culture etc.). In such case, technological surveillance would become, simultaneously, an element of social cohesion and of social control, superseding perceptions of insecurity and power imbalance.

5.1.4 Mobile Devices and Virtual Spaces

The virtual space, in which data from using a mobile phone are collected and monitored, appeared to be a space where the most ambivalent feelings and beliefs were revealed. The participants in all age groups demonstrated a rather detailed knowledge about technological surveillance of mobile phone data – through call lists as well as via GPS tracking. This was mainly understood as surveillance of private commercial operators for commercial reasons, e.g. marketing statistics or targeted advertising.

However, there appeared to be differences in the level of insecurity feelings produced by the knowledge of the surveillance of mobile phone data between the three age groups. In group III (age 45+), the predominant belief was that everyone who uses a mobile could be tracked, and these data would be under constant surveillance – but only the data of "suspicious" persons would be stored, not those of "normal" people. This specific belief seemed to provide them with a form of certainty and comfort.

Group II participants (age 25-44) believed that mobile phone data could be surveilled "for some security reasons" by the state and, then, retained for some time. Such assumed practice caused strong negative reactions amongst this group, participants expressing their lack of understanding why "their" data would also be stored. Here, the imbalance of power represented by state surveillance (using private surveillance data) was more strongly felt.

[3] Again, focus group participants did not at this point use the term "smart surveillance", but described the combination of surveillance technologies in their own words.

The youngest group (age 18-24), finally, revealed the strongest feelings of insecurity. They expressed their deep suspicion of constantly being under surveillance, and a specific uncertainty whether it was public or private entities who conduct surveillance in virtual space. Their in-depth technological knowledge and high usage of mobile appliances appeared to go alongside increased perceptions of lack of control.

5.2 Perceptions & Attitudes towards smart surveillance and dataveillance

One of the central tasks of this study was to research citizens' feelings and beliefs towards smart surveillance and 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 tap into the attitudes of the participants, the group was presented with an everyday scenario: a recorded telephone conversation between a job seeker and a public employee of the employment agency, during which increasingly more complex surveillance[5] becomes evident.

5.2.1 Feelings

Being asked immediately after having listened to this conversation, the focus group participants revealed feelings that ranged from "passive" discomfort to "active" anger. In group I (age 18-24), the participants predominantly expressed their rather strong discomfort. At the same time, however, some of them also expressed their expectation that people would adapt and get used to such extensive surveillance: *"If I called there like tomorrow and this happened I would be surprised. But if this happens gradually during like five, ten years, then, maybe, it won't be such a surprise"* (P4-I).

Group II participants (age 25-44) appeared to feel similarly, but they additionally explained their anger as being due to a *"complete loss of anonymity and freedom"* (P2-II) and the violation of human rights. Simultaneously though, despite perceiving it as a form of "physical" discomfort – *"as if I was naked"* (P6-II) – they would not feel helpless.

Group III participants (age 45+) were also uncomfortable with such a scenario. However, rather than linking it to a violation of perceived human or citizen rights, the scenario appeared to raise memories of practices of the former political regime which they linked to deep intrusion of privacy and, partially, individual helplessness.

At this point, it is tempting to form age group-related categories, linking them to generally different life experiences where younger citizens feel uncomfortable with extensive technological surveillance but are easier to influence and will adapt quicker. More mature citizens who are somewhat detached and, though unwillingly, accept the execution of governmental power, and an age group in-between which is most sensitive to citizens' rights and not so willing to accept or adapt to extensive technological surveillance. These observed differences may, obviously, not be as clear cut along age groups as described above; additionally, levels of acceptance will most probably vary with factors other than age.

5.2.2 Behavioural Intentions

[4] Clarke, R. (1997)

[5] The statements of the public servant allude to a drawing together of the jobseeker'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.

Focus group participants were not only asked for their feelings, but also for their resulting behavioural intentions had they to be faced with the extensive technological surveillance described in the scenario above. Here, is became evident that spontaneous feelings which may be influenced by life experience cannot be directly linked to an age group-specific behaviour – as in all groups there occurred three general "types" of imagined reactions:

(1) Passive or semi-passive. These participants described a deep insecurity which they expected to result in a health-affecting increase of stress or depression, potentially leading to a psychological disorder. They either *"wouldn't leave home for quite some time"* and *"be afraid to go amongst people"* (P9-I), stop using credit cards and pay more in cash, change their identity, move away either locally or even consider emigrating from their country, particularly the latter using sarcasm to mask their perceived helplessness.

(2) Taking legal action. These participants would attempt to either file a complaint with the public servant's superior (perceiving the experienced surveillance as data misuse by an individual rather that standard procedure), challenge the respective public authority by questioning why such comprehensive information was being collected, potentially asking another superior public institution for help, or directly file a criminal complaint against the employment office. All of them revealed a certain faith in the existing legal system and protection by law.

(3) Taking independent action: These participants were aware that the difficulty to know much about such surveillance and how the different surveillance methods and technologies worked together made it difficult to respond. Their strategy would be to take matters into their own hands, showing a strong self-assurance that they would be capable to *"find the leak and cut it off"* (P3-I).

5.2.3 Beliefs

5.2.3.1 Likelihood of smart surveillance and dataveillance

Regarding the likelihood of smart surveillance and massively integrated dataveillance being possible now or in the future, the focus group participants generally distinguished between technical, legal, and ethical aspects. Technically, the majority of participants in all age groups considered such scenario as likely given that the data themselves were perceived as already available: *"Everything can be found – the question is how someone will get to it"* (P8-I). However, it was also believed that, as yet, most surveillance would currently still be based on traditional technologies and fed into systems that were not interconnected, but the different sources would have to be pulled together manually.

Particularly group I participants (age 18-24) stated their belief that there was a foreseeable trend towards smart technologies increasingly being used. Similarly, in group II the participants considered it as a "not yet" situation – either due to the aforementioned need to establish automatic links between the different systems, or due to a perceived inefficiency of public institutions. Some participants of

group I and group III additionally expressed their opinion that the Czech Republic would not be technologically advanced enough to develop or apply smart surveillance – but *"there are countries where something like this exists"* (P1-III) – revealing a perception of complex surveillance as being done "somewhere else".

Specific legal aspects in the sense of protection against intrusive surveillance were solely mentioned in group I and related to the belief that surveillance (in online social networks or through databases) would only take place with the individual's informed consent; only one participant expressed his opinion that *"limits"* (P3-II) should be set by laws, rather than merely by ethics.

This statement, however, contrasts with the predominant opinion given – that the core reason why smart surveillance and massively integrated dataveillance would take place, or not take place, would depend upon individual and institutional ethics. Some participants believed that the scenario represented an *"individual ethical failure of the [public] employee"* (P5-II) rather than a systematic ethical failure of the state. But others felt that *"states [once] they have all the technologies, all the possibilities, and should they need it, they will use it for their interests"* (P1-III). Particularly group III participants related their belief of intrusive surveillance not being a question of available technologies but ethics and politics to their experiences with the former political regime: *"The old regime could help itself even without the use of other technologies. Back then, they were able to get similarly detailed information about one's private life – and there were no such technologies developed as today"* (P9-III).

5.2.3.2 Perceived effectiveness of smart technologies

Despite the comprehensive information on the different types of smart surveillance technologies and dataveillance methods provided by the focus group moderator prior to the audio-taped scenario, it seems that some participants found difficulty in understanding the exact nature of smart surveillance When referring to smart technologies, they mostly imagined CCTV with automated face recognition (AFR), occasionally linked with voice or gait recognition and noise detectors. Generally, participants expressed their opinion that smart surveillance has a stronger privacy impact than traditional surveillance methods, being even threatening to some, and as being only a "last resort" to fight crime, particularly in *"risky places"* (P5-I) and locations where many people accumulate:

> *"I think that the willingness to sacrifice the privacy is there, but I'd treat it as the last possible option […] First we should strengthen the police forces and work within the existing ways to protect order […] To sacrifice one's privacy just for the vision that it will be safer in the future is a very bad idea" (P10-I).*

During the discussion it seems that participants focused on the difference between automated and non-automated systems, equating non-automated technologies with traditional methods and automated with smart technologies. Taking up this simplifying perspective, the participants revealed rather ambivalent attitudes. On one side, there appeared a strong belief that automatised systems were more "objective" or *"impartial"* (P9-I) in their analysis: *"I'd definitely feel less vulnerable if let's say my*

movement, my type of walk, my facial expression was processed by a computer system than by a lady who has a degree in it and sits on the computer trying to see something from my face" (P5-I). Such belief could raise certain feelings of "comfort", because a machine would not have prejudices and *"does not care"* (P5-II), whereas conventional surveillance methods such as CCTV would raise feelings of "being watched" by a person.

However, once explicitly asked for their feelings about the automated procedures of smart surveillance technologies, the majority of participants expressed their discomfort, as they feared that a smart technology could also make systematic errors and furthermore such systems enjoy the trust of the police and the general public. In their discussions, it seemed that the participants were oscillating between on the one hand a desire to stay anonymous and not be surveilled by another human but rather by a "detached" technology, this being linked to a deep mistrust that their data could be *individually* misjudged through error or intentional misuse if surveillance is being carried out by humans rather than automated. And on the other hand, a vague feeling that a machine may not make individual errors, but carries the risk of *systematic* misjudgment.

Therefore, participants of all age groups ultimately stated that smart technology should not "decide" on its own, but there should always be a human operator who does the final evaluation. It also appeared that those participants who, initially, claimed that they *"don't mind"* (P2-III), revised their statements later when being probed; their initial attitude appeared to mostly be based on a belief that smart surveillance and fully automated decisions would not be technically possible anyway.

5.2.3.3 Citizen or state responsibility?

Additionally, some participants in groups II (age 25-44) and III (age 45+) expressed a strong belief that the likelihood of smart surveillance being implemented would depend on individuals taking responsibility not to make their private information publicly accessible. At the same time, though, participants outlined that it would be the state's responsibility not to mix up data gathered via (presumably justified) surveillance and unintentionally publicised private data. Information "packages" should have to be related to the respective public authority's task. Beyond governmental responsibilities, group III (age 45+) participants in particular revealed a strong belief in democratic processes. Technological surveillance as described in the scenario presented would only happen if *"the people let something like this happen to them – it depends on every one of us"* (P3-III), defining the task of keeping control over the usage of surveillance technologies as a citizen's duty.

Participants appear to hold contradictory beliefs here. Whereas, in the case of traditional surveillance technologies, participants of all age groups described throughout the focus group discussions vague feelings of loss of control and an imbalance of power, in the case of smart surveillance they seemed to appeal to political ideals, ethics and morality to achieve control. Thus, in the latter case, this may be interpreted as participants imagining a power balance between the state and its citizens as achievable which in the former case they had already accepted as an illusion.

5.3 Security-Privacy Trade-offs

5.3.1 General Acceptance and Non-Acceptance of Technological Surveillance

In order to gauge participants' perceptions vis-à-vis the security-privacy trade off, as well as their attitudes towards a number of specific smart technologies, a hypothetical scenario was presented to the group. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging. 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].

Reasons for acceptance, or non-acceptance, of technological surveillance depended strongly on the location of, and motivation for, such surveillance. In mass events, surveillance was mostly perceived as increasing safety, whereas, for example, extensive workplace surveillance was felt to be *"too much"* (P9-I). Generally, it appeared that feelings of being vulnerable were often linked to the insecurity of whether, when and where surveillance actually takes place. Only if it was possible to ascribe a distinct "caring function" to the entity undertaking the surveillance, e.g. the organiser of a mass event caring for attendees, or a bank caring for the assets of its clients, were feelings of security and comfort present.

Another reason for the acceptance of technological surveillance repeatedly indicated by the focus group participants was that they were "getting used to it". However, there were also indications of denial – *"no one can just monitor us – that just can't be"* (P6-I) – or assimilating unknown technologies to known everyday situations: *"It is as if there was a policeman"* (P1-III).

Otherwise, participants clearly stated their belief that crime prosecution and detection through surveillance would not provide or improve feelings of safety. The main reason given was the belief that technological surveillance does not prevent or protect against crime. Some expressed the opinion that technological surveillance would only help in fighting minor crime, whereas capital crime would be either planned very carefully or happen in unexpected situations – and in both cases surveillance would not work. Additionally, some participants expressed their fears that supposedly "harmless" data could be intentionally misused, or used for unexpected purposes that may induce harm, e.g. pictures or videos that reveal a medical condition becoming a reason for non-employment: *"Someone could recognize me and, based on the way I walk, [see] that I have a bad hip and he would not employ me based on this information"* (P4-II).

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

Ultimately, it was felt that systematic and comprehensive smart surveillance categorises each individual citizen as a *potential* risk – a process that was perceived as unacceptable and violating personal freedom:

> *"If I was in the position that […] there are cameras around and somebody records number plates and I am committing nothing and I am not in some sort of database, then I am calm. But when I am in a database with the DNA, fingerprints, and somebody labels me completely randomly or completely systematically as a possible risk – which already bears the risk that this does not have to be a person that has already been punished but could be only investigated, and now he is suddenly in the category 'possible risk' – well, here I am heavily beyond the border of personal freedom. And to 'brand' somebody like this and control him like this, that completely crosses the line" (P2-III).*

5.3.2 Acceptance of Different Technologies

Different types of surveillance technologies appeared to meet different levels of acceptance. In particular CCTV, sound detectors and automated license plate recognition (ALPR), being perceived as "impersonal surveillance" and collecting anonymous data, seemed to be widely accepted. The invisibility of these devices in combination with a generally high level of adaptation since they were first introduced appears to be contributing to this acceptance.

In contrast, the participants in all age groups revealed a strong discomfort with biometric surveillance. Whereas finding it acceptable to some degree for workplace access, registering all citizens' biometrics and tracking specific groups (elderly, children) – *"marked like sheep"* (P3-II) – was mostly deemed to be unacceptable: *"It's terrible to give DNA, [finger]prints, scan the iris, every person in the country – I can't imagine it"* (P8-I). Particularly surveillance in medical practices and surveillance of medical information databases triggered strong negative reactions. Overall, it appeared that the collection of any systematic or automated surveillance data that were felt to be closely related to the human body was not accepted, crossing a certain *physical* boundary of comfort.

Similarly, electronic tagging and GPS surveillance was perceived as violating privacy in a spatial dimension, because it was felt that such surveillance of an individual's movement was restricting a citizen's personal freedom. Although being accepted for specific reasons such as the surveillance of "criminal subjects", the infringement of a supposedly private sphere appeared to cause strong discomfort.

5.4 Surveillance Laws & Regulations

During the last part of the focus group sessions, the focus shifted to surveillance laws and regulations. A number of issues were discussed, including the effectiveness of surveillance laws and regulations, level of trust in the state and in private actors, length of data storage and issues of data sharing between different entities.

5.4.1 Effectiveness of laws and regulations

The focus group participants' feelings and beliefs about surveillance laws and regulations varied considerably depending on their age. Whereas some group I (age 18-24) participants felt *"quite protected"* (P10-I) through data protection legislation and consent procedures revealing a certain trust in the legal system, group II (age 25-44) participants felt only "partially" protected by law, holding the opinion that only once an incident had happened would law enforcement and legal protection become effective. Group III (age 45+) participants appeared to feel not assured by law, holding the attitude that, as long as there was human access to surveillance data there would be risk of misuse – independent from legal provisions.

5.4.2 Length of data storage

Being asked for their opinions about the length of surveillance data storage, the respondents of all age groups generally agreed that there should be differentiation between "unsuspicious" data from "normal" everyday surveillance and the storage of surveillance data which either document a crime, or derive from surveilling *"risky persons and risky areas"* (P5-I). For every day surveillance, the suggested storage was between one month and one year, with those suggesting the longer storage outlining that retrospective evidence for previously undetected crimes may be required. In the case of data obtained to document a crime or from the surveillance of people and areas considered to be risky, the suggested storage period was considerably longer, between two to five years.

Another distinction was made between surveillance data from traditional surveillance methods that would require storage until the material has been checked for any incidents, and data from smart surveillance where only the data with recorded incidents should be retained. Finally, some group II (age 25-44) participants expected biometric data not to be retained at all which confirms the aforementioned general discomfort about biometric surveillance.

5.4.3 Data sharing between different actors

Regarding the accessibility of surveillance data and information sharing between public and private entities, participants in all age groups appeared to draw a clear distinction between publicly and privately gathered surveillance data. Generally, they considered surveillance by public authorities as

more acceptable than surveillance by private entities, as they considered the general risk of data misuse within private companies to be greater. At the same time, though, they considered an actual misuse of surveillance data collected by public authorities as carrying a greater risk for the respective citizens than a misuse of surveillance data collected by private companies. Consequently, public authorities' potential sharing of surveillance information with others was perceived as *" dangerous – I would feel more endangered than in the case of a commercial group [sharing information]"* (P4-II). However, some participants related their attitude not so much to information gathered by the state being more sensitive than to holding already a certain expectation that private companies would make use of collected surveillance data anyway: *"When I compare these two spheres, I like more the commercial one. Like on Facebook, I am sharing my information voluntarily, and they use it afterwards […] When it comes to the social networks, I am counting on it to a certain extent"* (P1-II).

Additionally, group II (age 25-44) participants outlined their belief that unacceptable surveillance and/or misuse of surveillance data by the state could not be prosecuted, *"When the state does not protect me from itself […], then I have nowhere to go"* (P2-II). This power imbalance, as group III (age 45+) participants explained, would result in an even higher risk of data misuse when public and private entities were organisationally entwined. As much as such beliefs may be strongly based on these participants' experience and their country's political legacy, the secrecy surrounding the sharing of surveillance data between private and public entities appeared to raise general insecurity amongst all participants.

5. Conclusion: *"Marked like sheep"*

As outlined throughout this report, it appeared that the Czech focus group respondents did not have a clear idea about smart surveillance technologies, their usage, possibilities and limitations. Advanced technological knowledge as e.g. revealed by younger participants about online social networks and mobile phones, seemed not to go alongside an increased knowledge about surveillance technologies. If, to a certain degree, they imagined forms of smart surveillance, these were located in spaces with public or national security issues. There, technological surveillance seemed to fuel social cohesion, superseding perceptions of insecurity and power imbalance between the state and its citizens, although acceptance was mostly linked to a distinct "caring function" in distinct situations.

In general, an indiscriminate collection of surveillance data sources by any type of surveillance technology – smart or non-smart – was not accepted but perceived not only as the labeling of every citizen as a potential risk, but also as taking away humanity itself: becoming *"marked like sheep."* Here, particularly the systematic or automated collection of body-related or movement-related data appeared to cross the participants' physical boundary of comfort.

Ultimately, however, such violation of privacy and human rights was not so much ascribed to the automated decision-making of a somewhat "detached" surveillance technology, but to an excessive usage and incomprehensible complexity. In this context, the Czech participants revealed ambivalent beliefs: Whereas control and power balance in the use of traditional surveillance technologies had, possibly, become accepted as an illusion, there appeared some indication that concepts of smart surveillance may be perceived as still being under (democratic) negotiation between the state and its citizens, with both parties *sharing* the duty of keeping control.

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

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

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

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

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

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

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

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

- ☐ Yes
- ☐ No

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

- ☐ **Yes**
- ☐ **No**

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

- ☐ Yes
- ☐ No

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

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

APPENDIX B
DISCUSSION GUIDELINES (ENGLISH)

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

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

- *Start off the group discussion*

Read Out (one at a time):

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*

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:

Aims:

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

2. Explore the participants' experience of being

1. ***How is the information being collected:***
    a. ***Which types of technologies do you think are used to collect your personal information?***

2. ***What type of information is being collected:***
    a. ***What type of personal information do you think is being***

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

Presentation of MIMSI scenario to participants

[30mins]

- *To explore participants' understanding of the implications of MIMSI*

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

Item 4

Present the following hypothetical scenario to the group. A recording of the phone conversation can be prepared beforehand and presented to the group.

Phone conversation with the Customer Care Agent at the main branch of the Public Employment Service

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

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

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

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

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

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

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

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

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

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

***Customer Care Agent**: Let me check our system...what about Wednesday at noon? Oh wait a second! I just noticed that you have a doctor's appointment scheduled right at that time. And I'm sure you*

don't want to miss that since monitoring your cholesterol level is surely important! How about Thursday first thing in the morning at 9am?

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

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

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

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

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

Aims

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

1. Participants' first reactions including:

Possibility / impossibility of scenario
Acceptability / unacceptability of scenario

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

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

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

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

3a. What type of personal information do you find acceptable to being collected, used and / or shared?
3b. What type of personal information would you object to being collected, used and / or shared?

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

4a. What do you think about having your personal information collected, used and shared by the state?
4b. What do you think about having your personal information collected, used and shared by private entities (such as commercial ones)?

5. Participants'

5a. Do you think there are any benefits to having your actions

beliefs and attitudes on the benefits and drawbacks of being monitored	***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 whether these technologies effect privacy and hence revolve around the security - privacy trade-off*	***Item 5*** **During the next exercise, we will be discussing the following hypothetical scenario. Imagine the following scenario:** **Due to an significant increase in *<u>violent crimes</u>* in the capital city, including *<u>a spate of kidnappings and murders which seem random and unconnected</u>*, the state has decided to introduce CCTV surveillance in every public space, both those publicly owned (such as subways, public gardens and public conveniences) as well as those privately owned (such as shops, malls and taxis) which will enable automated face-recognition. In addition, all the cars passing through the main check points will have their number plates recorded. There are also plans to install sensors in all public areas which are able to detect loud noises such as in the case of someone screaming. All citizens will be required to have their DNA and fingerprints collected, and their iris scanned. The state has also decided that all citizens who are identified as presenting a possible risk to others should be electronically tagged to monitor and track their movements. For their safety, elderly people and children up to the age of 12 years will also be electronically tagged. All the data from these different technologies will be stored in linked databases administered by the police, who will be notified automatically should there be a cause for alarm and risk to any citizen.** ***Tell the participants to imagine the above scenario however with the following variations:*** **Variation 1: Even though a significant increase in violent crime is taking place throughout the majority of neighbouring cities, the city you reside in is not experiencing any increase in crime. However the state still decides to introduce the surveillance measures as a precaution.**

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

Aims:

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":

1. Security climate and level of threat

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

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

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

2. Deployment of specific technologies

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

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

2b. Which technologies do you consider <u>invasive</u> and as a threat to your privacy? Why?

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

3. Locations of deployment such as:
Airports
Malls
Streets

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

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

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

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

and use of data) *5. Length of storage of surveillance data*	***reassuring?*** ***5a. What do you think about the length of storage of surveillance data? Does it make a difference?*** ***To help you probe, provide the following examples to the participants:*** - ***Recordings of CCTV*** - ***The location and movement of cars*** - ***The storage of DNA, fingerprints and iris scans*** - ***The location of citizens who pose a risk to others*** - ***The location and movements of elderly people and children*** ***5b. If length of storage makes a difference, what would you consider as an acceptable timeframe?*** ***Running Total: 1 hour 35min***
Brief summary of discussion [5mins] ▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***Item 6 – Summing up session*** ***At the end of the focus group, it is helpful to provide a summary of the emerging points. Here you should aim at giving a brief summing up of the themes and issues raised during the discussion. After, you can ask for the following from the participants:*** - ***"How well does that capture what was said here today?"*** - ***"Is there anything we have missed?"*** - ***"Did we cover everything?"*** ***This brief session will give participants an additional opportunity to express their views and can also be used to elaborate on topics raised but not pursued at the time.*** ***Running Total: 1 hour 40 min***
Conclusion of focus group [5mins] ▪ ***Thank the participants*** ▪ ***Hand out the reimbursement*** ▪ ***Give information on SMART***	***Item 7 –Closure*** **With this last exercise our discussion has come to an end. May we take this opportunity to once again thank you for joining us and for sharing your opinions, experiences and thoughts.** ***At this point, hand out the reimbursements to the participants and inform the participants about the next steps.*** ***Give out more information about the SMART to the participants requesting such information.*** ***Total: 1 hour and 45 min***

APPENDIX C – DISCUSSION GUIDELINES (CZECH REPUBLIC)

Úvod	Briefing
Přivítání účastníků - *Uvítání účastníků* - *Rozdání jmenovek* - *Podpis formulářů souhlasu*	*Přivítejte účastníky hned, jakmile přijdou. Přidělte jim místo k sezení a jmenovku.* *Rozdejte formuláře "Souhlas s účastí na focus group („moderované skupinové diskusi")" a požádejte je, aby si jej přečetli a podepsali před zahájením focus group. Toto je velmi důležité pro to, aby účastníci rozuměli tomu, s čím souhlasili.*
Úvod [zhruba 10 min] - *Poděkování* - *Představení realizačního týmu* - *Účel* - *Důvěrnost* - *Trvání* - *Základní pravidla* - *Krátké představení účastníků*	**Vítejte na této focus group a děkuji za souhlas k účasti na tomto zasedání. Jsme rádi, že jste nám byli schopni věnovat tento čas ze svého nabitého programu podílet se tak na projektu SMART. Vaše účast je pro nás neocenitelná a moc si jí vážíme.** **Jmenuji se _____ a povedu tuto skupinovou diskusi. Pomáhat mi s tím bude _____, můj spolumoderátor, který bude vést o této diskusi zápis a bude ji nahrávat.** *Představte případné další kolegy, kteří jsou přítomni* **Naše sezení bude trvat mezi hodinou a půl a dvěma hodinami. Jelikož bude celé sezení nahráváno, chtěl bych Vás zdvořile poprosit, abyste mluvili jasně a srozumitelně. Vaše názory a myšlenky jsou pro náš výzkum velmi důležité a nechceme přijít o žádný z Vašich komentářů.** **Jak bylo již zmíněno, když jsme Vás kontaktovali původně s žádostí o účast v této diskuzi, tato focus group se zabývá tématem technologie a soukromí a je prováděna v rámci projektu SMART, který je kofinancován Evropskou Komisí. Pokud byste chtěli vědět více informací o projektu SMART, dejte nám prosím vědět a my Vás seznámíme s tímto projektem obšírněji v závěrečné fázi tohoto sezení.** *V této fázi je důležité neodkrývat účastníkům žádné další detaily týkající se obsahu této focus group aby se zamezilo ovlivnění následující diskuze.* **Jak jsme Vás již informovali, když jste si přečetli a podepsali formulář o souhlasu, vše, co bude nahráno během tohoto sezení, bude uchováno v tajnosti a bude anonymizováno – Vaše identita nebude tedy prozrazena. To znamená, že Vaše názory a komentáře budou sdíleny pouze s osobami, které jsou zapojeni do této studie a pak budou anonymizovány, než budou dále šířeny. Tedy, informace, které budou obsaženy ve zprávě, nebudou způsobilé Vás jakkoliv identifikovat jako účastníka této focus group. Abychom dosáhli tohoto cíle, bude Vám přiděleno číslo a toto bude následně použito ve zprávě o této focus group.** **Rádi bychom dosáhli toho, aby se každý v této skupině cítil natolik příjemně a pohodlně, aby mohl bez obav a naplno vyjádřit a podělit se o**

	své názory. Abychom tohoto cíle dosáhli, rád bych Vás všechny požádal, abyste se řídili těmito základními pravidly: ▪ **Rádi bychom slyšeli názory všech účastníků – zajímá nás názor každého.** ▪ **Neexistují správné či špatné odpovědi – dohodněme se tedy, že budeme vzájemně respektovat vlastní názory** ▪ **Ztište si prosím své mobilní telefony, aby nebyla diskuse přerušována.** ▪ **Je důležité, aby byly jednotlivé názory a komentáře vyjádřeny jeden po druhém, jelikož názor každého účastníka je důležitý. Pojdmě se tedy domluvit, že nebude hovořit více účastníků zároveň, jelikož by bylo jinak pro nás obtížné zachytit vše, co bylo vyřčeno v diskusi.** ▪ **Pojďme se jako skupina dohodnout na tom, že budeme respektovat soukromí každého z nás a to tak, aby se všichni cítili uvolněně a mohli hovořit naprosto otevřeně.** **Pokud by chtěl někdo z přítomných navrhnout nějaké další základní pravidlo, nechť je navrhne skupině nyní.** **Má ještě někdo před začátkem ještě nějaké další otázky či dotazy?** **Dobrá, dovolte, abychom naši diskusi zahájili tím, že se navzájem představíme, aniž bychom však odhalovali nějaké osobní informace. Představíme se popořadě, kdy se nám prosím představíte jménem a možná krátkou informací k Vaší osobě. Kolečko si dovolím zahájit já… *(krátce se představte)*** *Celkový uběhlý čas: 10 min*

Cíle	Diskusní témata a cvičení
Asociační cvičení **[Zhruba 5 min]** - *Hra na slovní asociace, která slouží jako aktivita k navození neformální atmosféry*	***Bod č. 1*** **Začneme krátkou hrou: Přečtu Vám slovo a požádám Vás, abyste řekli první věc, co Vás napadne, když slyšíte dané slovo. Zkusme si to na příkladu: Co Vás napadne jako první, když řeknu slovo "*jídlo*"? Pokud možno, snažte se přemýšlet v jednotlivých slovech, či krátkých frázích, tak abyste se vyhnuli dlouhým popisům.** *Předčítejte (jedno po druhém):* *Technologie, soukromí, národní bezpečnost, informace osobního*

- *Vytvořit spontánní asociace ke klíčovým tématům*
- *Zahájit skupinovou diskusi*

charakteru, osobní bezpečnost

Celkový uběhlý čas: 15 min

Diskuse o každodeních zkušenostech týkajících se sledování

[20min]

- *Zjistit zkušenosti účastníků se sledováním a jak jej vnímají*
- *Zjistit vědomost a znalosti účasntíků o různých sledovacích technologiích*

Bod č. 2

Pojdmě se bavit o něčem jiném. Přemýšlejte prosím nyní o situacích, během nichž máte pocit, že jste buď vy přímo nebo Vaše aktivity předmětem pozorování, jakož i o situacích v nichž si uvědomujete, že jsou o Vás shromažďovány informce. Začneme přemýšlením o aktivitách, které ve svém každodenním životě běžně vykonáváte. Projděme si nyní následující modelové případy.

Modelový případ 1: Supermarket

Jako první příklad si můžeme představit nákup ve Vašem obvyklém supermarketu. Můžete prosím sdílet Váš názor na tuto situaci?

Modelový případ 2: Cestování

Pojdmě se posunout k další situaci, tentokrát týkající se cestování. Co si myslíte ohledně leteckého cestování?

Modelový případ 3: Veřejné prostory (např. muzea, stadiony)

Nyní si představte, že jste navštívili veřejný prostor typu muzeum a nebo se účastníte veřejné události jako např. sportovní utkání nebo koncert. Jaké aktivity budou dle Vašeho názoru nahrávány?

Modelový příklad 4: Mobilní zařízení

Pojdmě nyní probrat poslední modelovou situaci – mobilní přístroje. Popřemýšlejte, kdy používáte mobilní telefon. Co je dle Vašeho názoru zaznamenáváno v tomto případě?

Cíle:

1. Prozkoumejte povědomí účastníků o sledovacích technologiích a

Pro každou položku, a tam, kde je to vhodné, do detailu prozkoumejte následující:

1. ***<u>Jak</u> jsou informace shromažďovány:***

    a. ***Jaké typy technologií jsou dle Vašeho názoru využívány ke shromažďování informací osobního charakteru?***

jejich znalost

2. Prozkoumejte zkušenosti účastníků se sledováním v jejich různých životních rolích

2. ***Co** je shromažďováno:*
   a. ***Jaké typy informací jsou dle Vašeho názoru shromažďovány?***

3. Prozkoumejte porozumění účastníků o tom, kde skončí jejich informace

3. ***Kdo** shromažďuje tyto informace:*
   a. ***Kdo je dle Vašeho názoru zodpovědný za shromažďování a zaznamenávání Vašich informací?***
   b. ***Kde si myslíte, že takové informace skončí?***

4. Prozkoumejte názory účastníků ohledně toho, proč jsou jejich aktivity a chování pozorovány, monitorovány a shromažďovány

4. ***Proč** jsou informace zaznamenávány, shromažďovány a uchovávány:*
   a. ***Proč jsou dle Vašeho názoru informace zaznamenávány a shromažďovány?***
   b. ***Jakým způsobem budou dle Vašeho nárzou tyto informace využity?***

Celkový uběhlý čas: 35min

Prezentace karet zobrazujících různé sledovací technologie a jejich aplikace
[10 min]

Seznámit účastníky s vybranými relevantními SMART sledovacími technologiemi a aplikacemi s cílem umožnit lepší pochopení a tedy

Bod č. 3

Ukažte účasníkům diskusní skupiny následující tři karty znázorňující skupinu různých technologií a aplikací. Karty budou obsahovat následující vyobrazení:

***Karta 1 – Rozpoznávání osob nebo událostí a sledovací technologie**: CCTV kamery s automatickým pohybem; Automatické čtečky poznávacích značek (ANPR) nebo automatická identifikace čísla vozidla (automatic vehicle number identification (AVNI)); a sledovací zařízení jako např. sledování mobilních telefonů a RFID (identifikace na rádiové frekvenci).*

***Karta 2 - Biometrika**: Biometrické technologie zahrnující skenování otisku prstů a duhovky; a automatické rozpoznávání tváře (automatic facial*

usnadění diskuze	*recognition AFR)* ***Karta 3 - Detekční zařízení předmětů nebo zboží:*** *Bezpečnostní rámy a rentegenová zařízení* *Celkový uběhlý čas: 40min*

Prezentace MIMSI modelové situace účastníkům

[30 min]

- *Vyzkoumat porozumění důsledků nasazení MIMSI technologií*

- *Zjistit pocity, přesvědčení a postoje účastníků, ohledně sdílení informací osobního charakteru*

Bod č. 4

Představte skupině následující hypotetickou situaci. Je možno připravit nahrávku telefonního rozhovoru dopředu a přehrát ji skupině.

Telefonní rozhovor se zaměstnankyní hlavní pobočky Veřejné služby zaměstnanosti (Úřadu práce)

***Zaměstnankyně**: Dobré ráno, zde Marie, jak se máte, pane Nováku? Očekávali jsme Váš hovor poté, co Vám již před více než měsícem skončil pracovní poměr.*

***Pan Novák**: Ehm..ano, to je ve skutečnosti důvod proč volám…*

***Zaměstnankyně**: Dobrá, nejsem překvapena, že voláte nyní…jak bylo na dovolená na Kypru? Věřím, že se Vaší paní a dětem líbilo letovisko, ve kterém jste byli…*

***Pan Novák**: Byla to skvělá dovolená…a jak to všechno víte?*

***Zaměstnankyně**: No, je to všechno v systému, pane Nováku…samozřejmě. Každopádně, pojďme se radši věnovat tomu, proč voláte a to je najití Vám nové práce…vzhledem k tomu, co stála Vaše rodinná dovolená a vzhledem k Vaší blížící se splátce na auto… nemluvě o té VISA platbě naplánované na 22tého tohoto měsíce…*

***Pan Novák**: I toto máte všechno ve Vašem systému?*

***Zaměstnankyně**: Ale samozřejmě Pan Nováku. Mimochodem, výborný výběr knih ve Vaší minulé online objednávce…sama jsem je četla a hodně jsem se toho dozvěděla.*

***Pan Novák**: Hmmm...ok...co se týče této nové služby ohledně hledání práce – potřebuji dodat moje aktuální foto?*

***Zaměstnankyně**: Ne pane Novák, o to již bylo samozřejmě postaráno! Máme spoustu Vašich aktuálních fotografií v našem systému. Což mi připomíná – na dovolené jste se pěkně opálil – skutečně Vám to sluší! Museli jste mít opravdu krásné počasí. Než zapomenu, ohledně té fotografie, preferujete fotku s brýlemi nebo bez?*

***Pan Novák**: Aha...no jo....bez brýlí bude lepší...takže, ohledně mé*

registrace…můžeme si domluvit schůzku někdy příští týden?

***Zaměstnankyně**: Momentíček, hned se na to podívám do systému…co takhle ve středu v poledne? Aha ne, pozor, jak jsem si všimla, to již máte naplánovanou kontrolu u lékaře. A je mi jasné, že ji nechcete zrušit, jelikož monitorování Vaší hladiny cholesterolu je pro Vás jistě důležité, jak by také ne. Co takhle hned ráno ve čtvrtek v devět?*

***Pan Novák**: Čtvrtek ráno zní dobře…musím donést ještě nějaké další podklady?*

***Zaměstnankyně**: Ne pane Nováku, veškeré potřebné informace máme již v našem systému.*

***Pan Novák**: To věřím...*

***Zaměstnankyně**: Díky za zavolání pane Novák a uvidíme se příští týden. Mimochovem, užijte si Vaše cappucino v Café Ole'...*

***Pan Novák**: Já...nashledanou...*

…

Cíle:

Po představení této modelové situace skupině se snažte zjistit následující

1. První reakce účastníků zahrnující:

1a. Jak byste se cítili, kdyby se něco podobného stalo Vám?
(Snažte se zjistit, jakou míru kontroly / pocit bezmoci by v takovém hypotetické situaci účastníci cítili.)

Možnost / nemožnost modelové situace

1b. Jak byste reagovali, kdyby se něco podobného stalo Vám? Co byste dělali?

1c. Je taková situace <u>možná/ nemožná</u>?

Akceptovatelnost / neakceptovatelnost modelové situace

1d. Je taková situace <u>akceptovatelná/neakceptovatelná</u>?

2. Přesvědčení a postoje účastníků ohledně toho, nakolik technologie ovlivňují nebo mohou ovlivnit jejich soukromí

2a. Do jaké míry se Vašeho soukromí dotýkají „samostatné" (jednotlivé) technologie?

2b. Do jaké míry se Vás, dle Vašeho názoru, dotýkají „smart technologie", tedy ty které zpracovávají data automaticky (nebo poloautomaticky)?

3a. Shromažďování, užívání a sdílení jakého typu informací

3. Přesvědčení a postoje účastníků pokud jde o informace typu: zdravotní dokumentace; finanční informace, fotografie a lokace

4. Přesvědčení a postoje účastníků ohledně shromažďování, užívání a sdílení informací osobního charakteru s třetími stranami

5. Přesvědčení a postoje účastníků ohledně výhod a nevýhod sledování

osobního charakteru je dle Vašeho názoru akceptovatelné?

3b. Proti shromažďování, užívání a sdílení jakého typu informací osobního charakteru byste měli výhrady?

4a. Jaký je Váš názor na shromažďování, užívání a sdílení Vašich informací osobního charakteru státem?

4b. Jaký je Váš názor na shromažďování, užívání a sdílení Vašich informací soukromými subjekty? (jako např. komerční subjekty)?

5a. Myslíte si, že monitorování Vašich aktivit a chování má nějaké výhody?

5b. Myslíte si, že monitorování Vašich aktivit a chování má nějaké nevýhody?

Celkový uběhlý čas: 1 hodina 15min

Reakce na modelovou situaci

[Zhruba 20 min]

- *Stimulovat debatu za účelem zjištění vnímání kompromisu "bezpečnost vs. soukromí" ze strany účastníků*
- *Zde by se neměla diskuse soustředit na to, zda tyto technologie zvýší bezpečnost, toto se mělo brát jako fakt. Diskuse by se měla soustředit na to, zda ty technologie, mají vliv na soukormí, a tedy se dotýkají kompromisu („trade-off) „soukromí vs. bezpečí",*

Cíle:
1. Pocit bezpečí a úroveň hrozby

Bod č. 5

Během následujícího cvičení budeme diskutovat tuto modelovou situaci. Představte si:

Kvůli významnému nárůstu násilné trestné činnosti v hlavním městě (a to i případy únosů a vražd, které se zdají být náhodné a bez vzájemné souvislosti) se vláda rozhodla nasadit sledovací technologie. Konkrétně se jedná o CCTV kamery na každém veřejně přístupném prostranství a to jak ve veřejném vlastnictví (metro, veřejná zeleň a veřejné toalety), tak v soukromém vlastnictví (obchody, nákupní centra a taxi), které umožní automatickou identifikaci pomocí tváře. Dále budou veškerá vozidla projíždějícími hlavními cestami identifikovány a jejich SPZ budou zaznamenány. Dále se plánuje, že na veřejných prostranstvích budou instalovány detektory, které budou schopny rozlišit hlasité zvuky, jako např. pokud někdo bude křičet. Všichni občané budou taktéž povinni odevzdat vzorek DNA a nechat si sejmout otisky prstů a naskenovat duhovku. Občané, kteří byli identifikováni jako potenciálně rizikoví pro svoje okolí, budou elektronicky označeni tak, aby mohl být monitorován a sledován jejich pohyb. Pro zvýšení jejich bezpečnosti budou starší občané a děti do 12 let taktéž elektronicky označeni. Všechny údaje z těchto monitorovacích prostředků budou uchovávány ve vzájemně propojených databázích spravovaných Policií, která bude automaticky notifikována v případě, že by vyvstala situace riskantní pro kteréhokoliv občana.

Nyní řekněte účastníků, aby si představili výše uvedenou modelovou situaci, ale v následujících variantách:

Varianta 1: I když došlo k výraznému zvýšení míry násilné trestné činnosti ve většině sousedních měst, v městě ve kterém bydlíte, k ničemu takovému nedošlo. Nicméně, stát se rozhodl zavést sledovací prostředky jako prevenční opatření.

Varianta 2: Celá země má obecně velmi malou míru kriminality. Vláda se ovšem rozhodla zavést preventivní sledovací opatření jakožto reakci na ojedinělý incident, při němž jednotlivec zahájil střelbu v nákupním středisku, následkem čehož zemřelo či bylo vážně zraněno několik lidí.

Během diskuze výše uvedeného modelového příkladu se snažte vyzkoumat následující faktory, a jak by mohly ovlivnit kompromis („trade-off") "bezpečnost vs. soukromí":

1a. Co v tomto modelovém případě by ve Vás vyvolalo pocit bezpečí?

1b. Co v tomto modelovém případě by ve Vás vyvolalo pocit zranitelnosti?

2. Využití specifických technologií

3. Místa nasazení jako např.
Letiště
Nákupní centra
Ulice

4. Existence právní úpravy sledování a dalších záruk (ve vztahu k shromažďování, uchovávání a užívání údajů)

5. Délka uchvovávání shromážděných údajů

1c. Byli byste ochotni obětovat svoje soukromí, pokud by byla úroveň hrozby rozdílná tak jako ve variantě 1 a 2 modelového příkladu?

2. Ze smart technologií jmenovaných v modelovém příkladu, tedy:

CCTV s automatickou identifikací pomocí tváře,
Automatické čtečky poznávacích značek vozidel (ANPR),
Senzory (se schopností detekovat hlasité zvuky),
Biometrické technologie (včetně otisků prstů) a
Elektronické označování (s využitím RFID)

2a. Které technologie jsou dle Vás akceptovatelné? Proč?
2b. Které technologie považujete za invazivní a ohrožující soukromí? Proč?
2c. Co si myslíte o těchto automatizovaných (nebo polo-automatizovaných) systémech, ve kterých je finální rozhodnutí učiněno systémem a nikoliv lidskou obsluhou?

3a. Na kterých místech je dle Vašeho názoru monitorování akceptovatelné? Proč?
3b. Na kterých místech je dle Vašeho názoru monitorování neakceptovatelné? Proč?

4a. Co si myslíte o právní úpravě regulující ochranu soukromí? Cítíte se díky ním chráněny?

4b. Existují nějaké záruky nebo podmínky, které by Vás uklidnily?

5a. Co si myslíte o délce uchovávání údajů ze sledování? Má to vliv na Váš názor?

Pro ulehčené výzkumu, poskytněte účastníkům následující příklady:
- ***Nahrávky z CCTV kamer***
- ***Lokace a pohyb vozidel***
- ***Uchovávání DNA, otisku prstů a skenů duhovky***
- ***Lokace občanů, kteří představují hrozbu pro ostatní***
- ***Lokace a pohyb starších osob a dětí***

5b. Pokud má na Váš názor vliv délka uchovávání, co byste

	považovali za akceptovatelný časový horizont? *Celkový uběhlý čas: 1 hodina 35min*

Cíle	Shrnující část
Krátké shrnutí diskuse [5mins] ▪ *Potvrdit hlavní probírané body* ▪ *Poskytnout další možnost dále rozvinout probrané*	***Bod č. 6*** ***Na konci focus group je vhodné poskytnout účastníkům shrnutí bodů, které vyvstaly v diskusi. Zde byste se měli zaměřit na stručné shrnutí probíraných témat a otázek. Poté můžete položit účastníkům následující dotazy:*** - **"Jak dobře se nám podařilo zachytit to, co zde dnes bylo řečeno?"** - **"Neuniklo nám něco?"** - **"Probrali a pokryli jsme všechno?"** ***Tato stručná sekce představuje další možnost pro účastníky prezentovat vlastní názory a může být využita pro rozvinutí témtat, které byla nadnesena dříve, ale která nebyla dostatečně probrána.*** ***Celkový uběhlý čas: 1 hodina 40 min***

Cíle	Závěr
Závěr focus group [5mins] ▪ ***Poděkování*** ▪ ***Rozdání náhrad*** ▪ ***Poskytnutí dalších informací o projektu SMART***	***Bod č. 7*** **S tímto posledním cvičení dospělo naše sezení do konce. Rádi bychom využili této příležitosti, abychom Vám ještě jednou poděkovali za to, že jste zde s námi dnes byli a sdíleli s námi své názory, zkušenosti a myšlenky.** ***Nyní rozdejte účastníkům náhrady a informujte účastníky o dalších krocích.*** ***Účasníkům, kteří na začátku diskuse projevili zájem, podejte více informací o projektu SMART.*** ***Celkový uběhlý čas: 1 hodina 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 Union. This focus group is being carried out by the *<insert name of institution here>* which is the co-ordinator for the SMART project in *<insert country here>.* The information obtained during this discussion plays a very important part in the research being carried out as part of this international project.

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

1.1. Commercial space

1.1.1. Awareness of different surveillance methods/technologies

1.1.1.1. CCTV

1.1.1.2. Loyalty cards

1.1.1.3. Financial monitoring (debit and credit cards)

1.1.2. Perceived purposes

1.1.2.1. Consumer behaviour research and marketing

1.1.2.2. Protection of property and goods

1.1.2.3. Safeguarding of payment procedures

1.2. Boundary (border) space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. CCTV

1.2.1.2. Biometric surveillance

1.2.1.3. Monitoring of personal data

1.2.1.3.1. Passport control

1.2.1.3.2. Passenger lists

1.2.1.4. Object detection devices

1.2.1.4.1. Metal detectors

1.2.1.4.2. X-ray

1.2.2. Perceived purposes

1.2.2.1. National security

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV with AFR

1.3.2. Perceived purposes

1.3.2.1. Prevention of crime

1.3.2.2. Timely detection, limitation and prosecution of crime

1.4. Mobile devices and virtual spaces

1.4.1. Awareness of different surveillance methods/technologies

1.4.1.1. Monitoring of call lists

1.4.1.2. Location tracking via GPS

1.4.2. Perceived purposes

1.4.2.1. Marketing and advertising

1.4.2.2. Security reasons

2. Perceptions and attitudes towards smart surveillance

2.1. Feelings

2.1.1. General discomfort

2.1.2. Physical discomfort

2.1.3. Anger

2.2. Behavioural intentions

2.2.1. Passive or semi-passive reaction

2.2.2. Active reaction

2.2.2.1. Legal action

2.2.2.1.1. File a complaint with the authority

2.2.2.1.2. Challenge the authority

2.2.2.1.3. File a criminal complaint

2.2.2.2. Self-reliance

2.3. Beliefs

2.3.1. Likelihood of smart surveillance and dataveillance

2.3.1.1. Technical aspects

2.3.1.2. Ethical aspects

2.3.1.3. Legal aspects

2.3.2. Smart surveillance versus traditional technologies

2.3.2.1. Understanding of smart technologies

2.3.2.2. Effectiveness

2.3.2.3. Adiaphorisation

2.3.2.4. Stronger perceived privacy invasion by smart technologies

2.4. 'Making sense'

2.4.1. Hope vs. pessimism that democratic processes will not allow such dimension of surveillance

2.4.1.1. Responsibility of state

2.4.1.2. Responsibility of citizen

2.4.2. Illusion of control

2.4.2.1. Belief that individuals are able to control their personal data

2.4.2.2. Belief that the state will safeguard citizens' personal data

3. Security-privacy trade-offs

3.1. Acceptance of technological surveillance

3.1.1. Feelings

3.1.1.1. Safety and comfort: the "caring" function of surveillance

3.1.1.2. Convenience and adaptation

3.1.1.3. Vulnerability: surveillance produces insecurity

3.1.2. General beliefs
3.1.2.1. Ethical dimension
3.1.2.1.1. Technological surveillance labels citizens as potential risks
3.1.2.1.2. Violation of personal freedom
3.1.2.2. Effectiveness of surveillance
3.1.2.2.1. Technological surveillance does not prevent or protect against crime
3.1.2.3. Too high risk of misuse
3.1.2.4. Locations of deployment

3.2. Perceptions of different technologies
3.2.1. CCTV, ANPR and sensors
3.2.1.1. Collection of "anonymous" data
3.2.1.2. Invisibility of devices
3.2.1.3. Comparatively high level of adaptation (part of 'everyday life')
3.2.2. Biometric Technologies
3.2.2.1. Strong perceptions of bodily/physical invasiveness
3.2.2.2. Contradictory perceptions between adaptation and invasiveness
3.2.2.3. Body data produce data doubles that are trusted more than the person herself, assessments (and discrimination) becoming putatively "rational"
3.2.3. Location tracking (GPS, RFID)
3.2.3.1. Limitation of freedom, citizen and individual rights
3.2.3.2. Acceptance for the tracking of "suspicious persons"

4. Surveillance laws and regulations
4.1. Feelings and beliefs
4.1.1. Effectiveness of laws and regulations
4.1.1.1. Level of trust in legal system
4.1.2. Expectations
4.1.2.1. Storage length of surveillance data
4.1.3. Information sharing between public and/or private entities
4.1.3.1. Public-public
4.1.3.2. Private-private
4.1.3.3. Public-Private – Private-public