Beliefs and attitudes of citizens in the Netherlands towards smart surveillance and privacy

Noellie Brockdorff[1], Christine Garzia[1], Melania Tudorica[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Faculty of Law, University of Groningen, Groningen, the Netherlands

January 2014

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

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

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

Table of Contents

1. Key Findings

This document presents the Netherlands 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 3 focus group discussions comprising of 22 participants from different age groups, which were held in order to examine the awareness, understanding, beliefs and attitudes of citizens towards smart surveillance and privacy.

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

The Dutch participants were highly aware of being under surveillance in different contexts including commercial, boundary and public spaces. When discussing these contexts, a wide range of surveillance technologies and methods was mentioned, including the use of loyalty cards with the aim of monitoring customer behaviour and the use of CCTV systems in order to observe citizens in various spaces. Overall, participants perceived customer surveillance as taking place mainly for security, marketing and advertisement purposes, while they perceived general citizen surveillance as occurring for reasons of national security and personal safety. Most participants were also aware of the extent of surveillance when using a mobile device and perceived this type of monitoring as primarily occurring for commercial and security reasons.

In order to gauge participants' attitudes and beliefs on massively integrated dataveillance, they were presented with a fictional scenario illustrating the massive integration of data. After an initial intense reaction, the possibility of integrated dataveillance actually occurring was discussed from a technical and legal perspective. To a lesser extent, some participants also mentioned ethical considerations. Even though opinions varied, most participants considered the massive integration of personal data as currently possible from a technical point of view, although not to the extent portrayed in the scenario. On the other hand, several participants questioned the occurrence of dataveillance since they perceived this practice unlikely due to current legal restrictions. Nevertheless, it appears that a few participants thought that this practice is already taking place. Moreover, in all focus groups, participants expressed a strong belief that the likelihood of massively integrated dataveillance taking place would also depend, in part, on citizens' self-responsibility in divulging their data, especially in the context of virtual spaces.
In addition to the likelihood of massively integrated dataveillance, participants also discussed its acceptability. Ethical considerations were raised by the participants, who perceived integrated dataveillance as unacceptable primarily due to privacy reasons. Overall it appears that acceptance was contingent on a number of factors, including purpose of use, whether consent was provided by the

citizen, whether data would be anonymised prior to being shared with third parties and the type of data to be stored and shared.

Participants' opinions on the effectiveness of smart surveillance varied, particularly in relation to the autonomous decision-making capabilities of smart technologies. A number of participants regarded automatized systems as more efficient in comparison to those requiring a human operator, whom they perceived as introducing an element of subjectivity in the decision-making process. On the other hand, others appeared to be sceptical of technology on its own without human agency. Overall, it appears that several participants preferred a combination of technologically-mediated surveillance and human operators in the surveillance process.

During the discussion of the "security-privacy trade off" scenario, while it appears that the use of video-surveillance and sounder sensors in public places was generally accepted, most participants considered the use of biometric technologies and electronic tagging as radical and extreme. It appears that, with the exception of CCTV systems, any increase in surveillance measures was perceived as increasing citizens' vulnerability. In addition to privacy reasons, participants argued that intrusive surveillance poses concerns relating to citizens' freedom and abuse of power by the state. Some also claimed that this could also result in a general criminalisation of citizens. As a result, most participants rejected the idea that an increase in surveillance would result in increased personal safety and public security and argued that security could never be fully guaranteed.

Participants were also invited to share their viewpoints on surveillance laws and regulations. It appears that some showed a lack of knowledge with regards to the content of the legislation. A predominant belief was that laypersons have difficulty in understanding legislation since it is vague and lacks clarity. In line with this, some participants, specifically from Group 1 (18-24 years), argued that legal information should be provided to citizens in a straightforward and transparent manner. Nevertheless, others pointed out citizens' lack of initiative in getting informed. In relation to the effectiveness of legislation, opposing views were evident; while some stated that they do feel protected by current legislation, several others expressed their misgivings regarding its effectiveness. In relation to the length of time surveillance data should be stored, expectations were varied and participants suggested a number of criteria which had a bearing on storage length of surveillance data, including purpose of use, type of data and locations under surveillance.

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 Netherlands is Rijksuniversiteit Groningen (RuG).

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 Netherlands. Other separate reports are available for Austria, Bulgaria, Czech Republic, France, Germany, Italy, Malta, Norway, Romania, Slovakia, Slovenia, Spain and the United Kingdom.

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

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

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

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research project. The focus groups in the Netherlands were carried out on the 6th March, 2013; 11th March, 2013 and 14th March, 2013. The composition of the groups held in the Netherlands 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 Dutch 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 Netherlands is based on a total of 22 and the composition of all three groups is depicted in the following table:

Participant number	Group 1 – 18-24 years	Group 2 – 25-44 years	Group 3 – 45+ years
P1	F	M	M
P2	M	M	F
P3	F	M	M
P4	M	M	F
P5	F	F	M
P6	F	F	F
P7	-	M	M
P8	-	M	F
Total	**6**	**8**	**8**

In general the atmosphere of the three groups was rather similar and was described by the moderators as friendly and informal. The overall flow of discussion was smooth in all three groups. In particular, Group 1 (18-24 years) and Group 3 (45+ years) participants were described as enthusiastic and very involved with the discussion and were especially willing to listen to each other.

With regards to the discussion in Group 2 (25-44 years), although this was considered as flowing, it appears that one of the participants (P1) was rather dominant and talkative. Due to this, the moderators stated that the discussion got off-track and it proved difficult to get the discussion back on track since this particular participant would insist on finishing his point. Moreover, it appears that he interrupted the other group members rather frequently and this behaviour seems to have intimidated a number of participants and might have discouraged them from contributing to the discussion. In particular, the input of three participants (P4, P5 and P7) was rather limited since it proved difficult to get them involved in the discussion.

5. Results

5.1 Surveillance Technologies in Different Spaces

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

5.1.1 Commercial Space

The certainty of being under surveillance *"for multiple purposes"* (P6-III) was noted throughout the discussion of surveillance in a commercial context: "*I know for sure one is being monitored at the supermarket"* (P5-I). Video-surveillance systems and the use of loyalty cards were perceived as the predominant methods through which consumers are monitored, while less frequently mentioned methods of surveillance included financial monitoring.

In contrast to other methods of surveillance which might be considered as covert, it was pointed out that the use of cameras was rather obvious: "*In a lot of shops there are signs like 'You are being monitored' or you see this screen when you walk in and you see yourself coming in. That's just to show that you're being seen"* (P5-I). Participants regarded video-surveillance as having a number of purposes including those related to security; here they mentioned the prevention of crime, such as shoplifting, as well as the investigation of crime: *"a robbery could have taken place, of course then they are watching it"* (P6-I). However, participants were quick to point out that such monitoring *"is not all [about] security"* (P7-III) and proceeded to argue that cameras are also utilised in order to monitor consumer behaviour for other reasons, including a better product and shelf organisation in order to optimise the commercial establishment's turnover:

> *"[…] they monitor the way people move about and they base their entire set-up on this. Obviously, nothing is left to chance at a supermarket, even the smallest detail has been figured out […] They monitor how you walk and perhaps your eye movement and direction, what catches your eye first, that sort of thing" (P8-II)*

Loyalty cards were perceived as enabling commercial establishments *"to keep track of what you actually buy"* (P6-I) and *"to register certain patterns"* (P6-II). A number of participants argued that the attractive incentives linked to the use of loyalty cards, such as providing *"special deals"* (P6-I) to customers, in practice served this primary and rather covert purpose: *"[…] and the fact that it's beneficial has a reason, it's not just to give you a discount but it's there to monitor your buying pattern"* (P8-II). Such monitoring was regarded as having several purposes, mainly those relating to advertising and marketing research. In

relation to this, the collection of customer data was perceived as being a *"goldmine"* (P1-II): *"[…] these are only being saved [in order] to make more money I think"* (P7-II). Such data was regarded as being highly profitable due to the belief that not only could it be used by the commercial establishment collecting it, but in turn it could also be sold to third parties such as marketing companies or other entities involved in scientific research such as universities. However, in the latter case, some participants argued that such data would be anonymised prior to being shared or sold: *"[…] But in any case personal data, if there are any, will certainly be eliminated. They just provide these data. In a sense like, this many people buy this product and this many people buy that product […]"* (P1-I).

5.1.2 Boundary Space

In the context of border control, the discussion mainly focused on an airport setting as a boundary space. Surveillance at land borders was also briefly touched upon, which was overall perceived as being considerably less rigorous in comparison to surveillance at airports.

Surveillance in airports was considered as ubiquitous and inescapable: *"So no one, apparently, can be invisible when it comes to these things […] that is impossible unless you live in a cave"* (P8-II). At the outset, some participants argued that surveillance in the context of air travel is already underway "*when you book your flight"* (P4-I). In this context, participants perceived national security and passenger safety as being the predominant purposes of surveillance: *"I think that safety, security, plays the biggest part"* (P3-I). To a much less extent, some participants additionally mentioned commercial motivations and functions related to the collection of statistics, albeit they did not discuss this in detail.

In line with the pervasiveness of surveillance in this space, a variety of surveillance methods was mentioned by the different groups. The use of video-surveillance, including traditional CCTV systems and smart CCTV with automatic facial recognition (AFR), as well as biometric technologies were considered as being widespread in this context. Participants also mentioned a number of object and product detection devices, such as luggage controls, metal detectors and full body scanners as well as the monitoring of personal data via passport control, passenger lists or the airline booking system. Some participants also alluded to the massive integration of data from different databases: *"systems will also be joined"* (P1-I). In addition to technological surveillance, some participants also mentioned surveillance by staff who are *"trained to look out for certain behaviour"* (P6-I) and also the use of sniffer dogs. Overall it appears that participants were generally aware of being surveilled by a variety of entities with each having *"their own interest"* (P1-III). These included airport security services, commercial entities such as airline companies, different state authorities such as the Military Police, as well as foreign governments.

As already mentioned above, participants perceived national security and passenger safety as major purposes of surveillance at airports. In particular, participants mentioned a prevention function by the prior identification of *"high risk"* individuals: *"they often do select people who are a high risk or this or that […] or they lead people who they'd like to examine a little closer to a special little room and there*

they further interrogate these people" (P1-I). Others additionally mentioned that surveillance data could serve as evidence *"in case something happens with the plane"* (P2-I). Participants also mentioned the possibility that surveillance can also be used as a means to control national borders, for instance in order to detect individuals, such as criminals, who are prohibited from entering or leaving the country.

Some participants argued that the extent of surveillance at airports is dependent, in part, on the country in question:

> *"[…] and obviously you move from one place to the next, they have not discovered anything earlier and then you arrive in London and there everything is even more thorough, what's this, what's that etc. The British are more paranoid even, and it gets worse in Australia and even worse in New Zealand. It does depend on the country"* (P8-II)

5.1.3 Common Public Spaces

In common public spaces, such as stadiums and town squares where mass events like concerts are organised, participants mentioned a range of methods through which surveillance occurs. All focus groups mentioned the use of CCTV as a primary means of surveillance in this context and, additionally, some participants also pointed out the possibility of being inadvertently recorded by any television cameras filming the event. The monitoring of personal data via the purchase of tickets and ID checks upon entrance to the event was also mentioned during the discussion. Moreover, some participants from Group 3 (45+ years) mentioned surveillance via the use of audio equipment. Participants from Group 2 (25-44 years) discussed the possibility that individuals can easily generate surveillance data themselves through the use of personal mobile devices equipped with cameras: *"[…] you record one another […] when you take a picture of someone then there will be 30 others caught on camera"* (P6-II).
In addition to the above mentioned technological surveillance, all groups mentioned the presence of security officers and law enforcement personnel, including plain clothes police officers, in order *"to keep an eye on things"* (P5-I). For some participants, the human element was considered necessary: "*[…] but certainly when there's such a crowd of people, you need people to be physically present in case of escalations and things like that […]"* (P1-I).

In general, the predominant function of surveillance in public places was perceived as being public security and citizen safety. Data was believed to be collected by state authorities, primarily law enforcement agencies, as well as by private entities, mainly the event organisers and private security companies. Participants discussed a number of different purposes including the timely identification of trouble makers so that necessary action could be taken. In relation to this, some participants believed that such data would be stored in order to avoid future incidents: *"[…] because if there is someone causing problems they would like to prevent that next time"* (P6-I). Additionally, others mentioned that surveillance data could serve as evidence during the investigation of incidents: *"I think it is mainly to collect evidence to investigate when things, well, especially when things go wrong, then at least you can see what, who has done what"* (P2-I).

5.1.4 Mobile Devices and Virtual Spaces

Participants from all groups appeared to be aware of the extent of surveillance when making use of a mobile device and mentioned a range of methods through which technologically-mediated surveillance occurs, or can potentially occur, within this context. The most frequently mentioned method was location tracking through GPS: *"they are able to trace you anytime if they would want to do so"* (P4-I). Others mentioned the monitoring of call lists and the recording of conversations, whilst significantly fewer participants discussed the collection of data through the use of Bluetooth and Wi-Fi networks as well as via smart phone applications.

In general, it can be noted that the perceived purposes of surveillance data differed according to the type of data gathered. Information pertaining to call lists and other data relating to billing systems was mainly understood as surveillance by the mobile phone provider for *"purely commercial"* reasons:

> *"[…] they need to register where this phone is plugged in, what the number is, the number it's calling, by what number it is being called, how many seconds. That's what you base the invoice on" (P4-II)*

In addition to billing, other commercial reasons mentioned by some of the participants included the generation of statistics used for marketing and advertising purposes; such data was deemed as rather valuable for the mobile phone provider: *"There is a lot you can analyse from unprocessed data"* (P1-II).

Other types of surveillance data, primarily the recording of conversations and location tracking via GPS, were perceived as being used for security-related functions. In general, participants mentioned such data as providing the means for law enforcement personnel to prevent and fight crime, such as the identification of individuals who *"behave suspiciously"* (P3-II). Participants also mentioned functions related to crime investigation; in particular one participant narrated the following first-hand experience which appears to have left a certain impression on him:

> *"[…] after three weeks I received a text message from the police saying that I had been near Breda on that specific day and if I had, because a crime had been committed, and apparently this had happened near the train track, whether I had seen anything. So this was three weeks after. So they are able to tell from the signal your phone is spreading that you were near at that moment and I did think that was kind of creepy" (P2-I)*

In such cases as illustrated above, the participants perceived the provision of data by the mobile phone provider to law enforcement agencies not as a *"standard procedure"* (P1-II) but as one requiring a warrant:

> *"I know the police they can just…they'd have to do this through court, but they can just ask at the telecom provider like, gosh, this person has an account at your company, would it be possible to give us the records on where he has been over the past five days? And where he is now? They can give these details […] (P1-II)*

In addition to the likelihood that customer data is passed on to the police, participants additionally mentioned other third parties with whom such data could be shared, including advertisers, phone manufacturers and other government entities. Although some participants said that legislation provides limitations in this regard: *"[…] they're being restricted by law as to whom they can make it available and to whom they can't*" (P1-II), others believed that their personal information ends up "*all over the place"* (P2-I). These participants were keen to point out that the collection of such extensive surveillance data is a double-edged sword: "*[…] it can be used for security reasons, but it can also be turned around and used against you. That's kind of the danger of it I think"* (P4-I). In particular, some participants mentioned their concern with regards to data theft: *"The question is: who can steal these?"* (P7-II).

5.2 Perceptions & Attitudes towards Smart Surveillance and Integrated Dataveillance

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

5.2.1 Feelings

After having listened to this conversation, the focus group participants revealed feelings which predominantly indicated an extreme sense of discomfort: likened to George Orwell's 1984[4], this *"oppressive"* (P5-II) scenario evoked a range of feelings which included feeling *"powerless"* (P7-II), *"very uncomfortable"* (P2-III) and *"very unsafe"* (P6-III). Moreover, for many participants, this *"Big Brother"* (P7-II) scenario appeared to elicit a deep sense of helplessness: *"You're no longer in control of anything"* (P2-III). Similarly, another participant feared that citizens would gradually become resigned to intrusive surveillance: "*[…] there is nothing you can do about it. That's the problem. At some point you let it happen […]*" (P8-II). A few participants stated that they would feel angry should they have experienced this first hand.

5.2.2 Behavioural Intentions

In addition to asking about their feelings upon listening to this conversation, participants were also asked for their resulting behavioural intentions, which were somewhat varied. While some participants suggested a rather passive reaction involving some kind of immediate withdrawal from the hypothetical situation, such as hanging up the phone, others claimed they would have questioned the civil servant about how their personal data was obtained: *"At least I would have asked how they managed to get all this information"* (P5-I). One Group 2 (25-44 years) participant stated that experiencing such an *"extremely bizarre situation"* (P1-II) would compel him to establish a lobby group to campaign for privacy rights.

One participant from Group 3 (45+ years) stated that such an incident would be cause for reflection: *"Afterwards I would really ask myself 'how can I protect myself better?'"* (P6-III) Here, some of the group

[2] Clarke, R. (1997)

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

[4] The author George Orwell published the book "Nineteen Eighty-Four" in 1949, which describes a dystopian vision in which government surveillance is omnipresent.

participants suggested certain self-protection strategies in relation to one's use of technology: *"Well, that is possible, [if] you no longer use your card to pay and no longer use your mobile phone"* (P7-III). At the same time, however, the same participant expressed in a rather joking manner that shunning the use of technology would not only be unrealistic but also impractical: *"Yes, then we go back to the old days, let's do it all through post and pigeons again […] and horse and cart (laughs)"* (P7-III).

5.2.3 Beliefs

5.2.3.1 Likelihood of smart surveillance and integrated dataveillance

Regarding the likelihood of whether or not smart surveillance and massively integrated dataveillance are possible (currently or in the future), the focus group participants generally distinguished between technical, ethical and legal aspects.

Generally, the development of massively integrated dataveillance was perceived by most participants to be certainly possible from a technical aspect, albeit not to the extent as portrayed in the scenario, which was considered by some as *"quite extreme"* (P8-II) and *"heavily exaggerated"* (P6-III). A minority of participants argued that to a certain degree the massive integration of data from different sources is *"already a reality"* (P5-III): *"Some of it is already happening […]"* (P8-II). Nevertheless, although technically possible, several participants questioned the likelihood of massively integrated dataveillance from a legal perspective: *"[…] all these data are somewhere, only the freaky thing is that there must indeed be someone who links it all together, I think it's possible, it isn't legal but I do think it's possible"* (P2-I). Moreover, ethical considerations were brought up by the participants who perceived the massive integration of data as unacceptable primarily due to privacy reasons: *"They just know everything about you. I mean what you are doing at home, at work, everything"* (P5-II).

In all focus groups, participants expressed a strong belief that the likelihood of massively integrated dataveillance taking place would depend to a certain extent on individuals' self-responsibility in divulging their personal information: *"[…] but it does depend on how you take care of your own data, doesn't it?"* (P5-I) Several participants argued that the blame rests with the individuals themselves if they *"voluntarily divulge"* (P1-II) their personal data in a careless manner. The discussion here mainly revolved around self-responsibility in the context of virtual spaces. In fact, some participants made sense of the scenario by linking it to the *"rather stupid"* (P2-III) use of online media such as social networks: *"[…] an important element of this now is probably the social media where we are the ones tainting our privacy, voluntarily, without realising it ourselves"* (PI-II). Some participants conveyed several concerns regarding *"the danger of these social media"* (P1-III). While some expressed unease that when sharing personal data online, *"you don't realise, so to speak, where it all ends up"* (P6-III), others voiced their concerns about the permanency of data traces: *"All that is posted through social media, mainly Facebook and Twitter, just stays on the internet. And it won't disappear"* (P3-I). Once

again, in relation to this, some participants emphasised the responsibility of the individual: *"[…] but you have to be aware of this and be careful*" (P5-I).

5.2.3.2 Acceptance of smart surveillance and integrated dataveillance

After discussing the likelihood of massively integrated dataveillance, the participants also discussed its acceptability. As mentioned previously, an overwhelming majority of participants regarded the scenario as clearly unacceptable since they perceived it as tantamount to a *"violation of privacy"* (P4-I). In relation to this, several participants agreed that technology has a negative impact on privacy and that technological advancements are *"putting privacy under more and more pressure"* (P1-III). At the same time, however, some participants argued that surveillance is, to a certain extent, undergoing a process of normalisation: *"You are aware of it, but […] you just no longer pay attention to it"* (P8-II).

Overall it appears that participants' acceptance of massively integrated dataveillance depended on a number of factors. In general, it seems that a major factor influencing acceptability was purpose of use: "*You just want these data to be used for the purpose they were meant to be used for"* (P1-I) Here, participants mentioned several uses which they considered as acceptable, including research uses such as those related to the analysis of consumer behaviour, especially since they perceived such data as being anonymised prior to being shared with third parties:

> *"[…] if the personal data are being deleted so it's purely about unprocessed data […] then it's fine […] when you remove that, then naturally you can save a lot of data, it's fine to share, no problem at all" (P1-II).*

Additionally, others stated their acceptability of dataveillance vis-à-vis crime-related purposes, such as the investigation of money laundering, as well as in relation to general security measures: *"As long as it is [done] to increase and guarantee security, I am okay with it […]"* (P3-II). Dataveillance was also perceived by some participants as acceptable in cases where it was considered as facilitating user convenience: *"In a way it is kind of handy, isn't it?"* (P4-I) Nevertheless, some pointed out a number of risks, in particular that data could potentially be used for *"malicious purposes"* (P1-II).

Moreover, it appears that whether consent was given by the individual whose data was being shared was also a factor influencing the participants' acceptance of dataveillance. Some participants argued that unless *"permission to do so"* (P5-I) is expressly given, the sharing of personal information would be deemed as unacceptable. Indeed, the practice of data sharing without the user's consent was perceived as infuriating by some:

> *"Don't you think it's annoying that they do this behind your back? You do receive an email and coincidentally you need something like that, but don't you wonder like how the hell did they find my e-mail address, don't you feel like that?" (P1-II)*

Dataveillance on the internet was also brought up, especially by Group 1 (18-24) members. In particular, they discussed the customisation of content on the internet, which seems to have been subject to mixed reactions. It appears that several participants perceived this as an invasion of privacy and thus objected to such a practice, even though they assumed that this was an automated process: *"you feel like someone is watching along in some way […] although it is probably more [the case] that it is being triggered by words but yes I think that is annoying as well"* (P1-I). On the other hand, others did not seem particularly bothered by the customisation of content: "*Personally I do like to get brochures that are of use, new clothes for skiing […] that's perfect, then I am like, that's fine, at least these are things that I need on a regularly basis"* (P2-II).

Another aspect which had a bearing on the acceptance of dataveillance was the type of data to be stored and shared. Although there were slight differences in the opinions of participants, some general trends emerged. Overall, it appears that participants agreed that *"as little as possible"* (P4-I) personal data should be made public. The most confidential personal data included pictures, location, financial information as well as medical and health data. Nevertheless, it appears that in specific situations, especially in potentially life-saving circumstances, the use of certain types of confidential data, such as medical data, was considered as justified since "*it makes it easier to respond to emergency situations"* (P5-I). A similar argument was suggested in relation to location-tracking:

> *"[…] when for instance you say I don't like it when everyone knows where I am, yes in that case I would be against it, but the moment you're being kidnapped for example, then I am sure that you're quite happy that everyone knows you are there at the moment" (P3-I).*

Lastly, the participants, in particular Group 1 (18-24 years) members, discussed their attitudes towards the collection, use and sharing of data by the state and by commercial enterprises. Attitudes on this issue were noticeably mixed; whereas some participants were of the opinion that the state was more trustworthy in this regard: *"I think the state offers a little more guarantees […] the state could have certain purposes on the one hand but probably also a lot of good ones"* (P5-I), others, especially participants belonging to Group 1 (18-24 years), did not show much trust in the authorities: *"[…] I am not really confident that my data are being kept safe […] it is uncertain what happens to it"* (P2-I). In relation to private entities, overall participants expressed a lack of trust: "*I do think that individual entities will be quicker to part with their files containing these data to who knows who […]"* (P2-I). When data sharing occurs amongst private actors, not only did participants perceive a stronger violation of privacy, but they also regarded such practices as resulting in increased risks: *"I think that with private entities a lot of bad things happen, perhaps especially with private entities"* (P5-I).

5.2.3.3 Perceived effectiveness of smart technologies

Issues of effectiveness were also mentioned by the participants, who primarily discussed the automatic decision-making process of smart technologies. It appears that the issue of automation brought up

mixed feelings and beliefs amongst the participants. Firstly, the participants differentiated between decisions taken by humans and those taken by automated technologies. In this regard, a number of participants perceived automatized systems as being *"less prejudiced"* (P8-II) and *"impartial"* (P7-III) since there is no human agency involved. These participants, in particular Group 3 members (45+ years), argued that humans introduce an element of subjectivity which negatively influences the decision-making process:

> *"[…] each person approaches an incident in a different way […] it's often the case that when you encounter a human being they are already biased so through this bias you get a wrong picture of where and how or what, you see? And if you let technology take care of this, so to say, then it's all equal" (P7-III).*

Additionally, others argued that humans are also easily influenced: *"[…] people are easier to influence, they act on their emotions, and I am not sure if that is always a good thing"* (P3-I). On the other hand, some participants appeared to be sceptical and distrustful of technology on its own without human agency. These participants appeared to challenge the decision-making capabilities of smart technologies and argued that the final decision should be *"executed by a human being"* (P6-I). It appears that these participants, mainly from Group 1 (18-24 years) and Group 2 (25-44 years) preferred the use of both technologically-mediated surveillance and human operators in the surveillance process: *"[…] perhaps this combination of machine and a human being is still the strongest combination"* (P5-I).

5.3 Security-Privacy Trade-offs

5.3.1 Acceptance of Technological Surveillance

In order to gauge participants' perceptions vis-à-vis the security-privacy trade-off, as well as their attitudes towards a number of specific smart technologies, a hypothetical scenario was presented to participants. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging. The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[5].

When discussing the scenario, the majority of participants had a very intense reaction, perceiving the use of all the aforementioned surveillance measures in conjunction as *"really frightening"* (P6-III) and as particularly excessive: *"I think it's all quite extreme"* (P4-I). Participants from the different age groups argued that with the introduction of intrusive surveillance, a democratic state could easily develop into a totalitarian regime: *"this is obviously how you completely move towards a police state"* (P4-I). In fact, rather than enhancing feelings of personal safety, the security measures portrayed in the scenario resulted in feelings of discomfort and insecurity amongst most of the participants: *"You are just vulnerable"* (P7-III). Moreover, some participants also feared that once such measures are introduced, the intensification of surveillance would undoubtedly continue to escalate: "*then the next step to something else is easily taken"* (P4-I).

A number of reasons can be attributed to this increased sense of insecurity and vulnerability. Firstly, a number of participants expressed concern at the way that surveillance measures affected their privacy, perceiving surveillance technologies as providing a means through which one is *"constantly being spied upon"* (P2-III). In relation to this, participants appeared troubled at the possible normalisation of intrusive surveillance: *"at some point everybody will think that it is normal* (P5-III).

While for several participants privacy was considered as more important than security, there were participants who in addition revealed other concerns. Issues such as *"freedom"* (P2-II) and *"power"* (P1-II) were underscored by participants mainly belonging to Group 2 (25-44 years). The use of intrusive surveillance was perceived as creating the ideal conditions for *"restricting citizens' freedom"* (P2-II) and as providing the perfect opportunity to those *"who want to exert power over others"* (P8-II). In fact, some conveyed their concerns that all the data gathered would be administered by the police force: *"the fact that everything is being managed and retained by the police. That scares me"* (P4-I). Ironically, one of the participants said *"I'm more afraid of the authorities here than I am of criminals"* (P1-I). Such a

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

perceived power imbalance between the citizen and the state resulted in a feeling of extreme vulnerability:

> *"[…] if you do want to create a police state then this is the first step. What happens here is that you give people the exact means to exert ultimate power over you. That is just the silliest thing you can do. So this isn't safe, you just put your life in other people's hands" (P1-II)*

In particular, the participants appeared concerned that the focus of surveillance could shift from monitoring criminals to observing all citizens. They argued that an intensification of surveillance would not only represent a threat to privacy and freedom but also result in a general criminalisation of citizens where *"everybody is [considered] a suspect"* (P1-II) right from the outset:

> *"[…] even before you have violated the law, you are already being tracked by the government and this bothers me. Purely the fact that I am a citizen, purely the fact that I have human rights, makes it possible for me to violate the law, even though I don't have any intention of doing so. I think that's just weird. Presumption of innocence does not exist any longer" (P6-1)*

In spite of a marked increase in crime portrayed in the alternative versions of the scenario, participants were still of the opinion that extensive surveillance measures could not be justified, with only a minority expressing their confidence in surveillance measures and a corresponding willingness to sacrifice their privacy following an increase in crime: "*Well I'd rather sacrifice my privacy when there's a risk of me being shot whilst walking out on the streets or something. So in that case I'd rather have no privacy"* (P2-I). While the latter participants seemed to appreciate the caring function of surveillance, it appears that the majority of participants, upon reflection, showed a rather critical and questioning attitude towards the use of surveillance.

Overall, it appears that most participants were not willing to sacrifice their privacy for increased security: *"I think that perhaps it might provide a sense of security but I think it is absolutely not worth it"* (P5-I). The predominant belief amongst participants was that security could never be fully guaranteed: *"[…] even if you would do all these things and everyone would be following the rules neatly […] even then we wouldn't prevent everything"* (P1-II). A number of participants doubted and challenged the notion that technological surveillance was the best solution to reduce or eliminate crime since the use of surveillance was perceived as treating *"the symptoms [rather than] the cause*" (P1-II).

Although most participants acknowledged that the use of technology could be somewhat useful for purposes of investigation*: "At best you will be able to see who it was, in retrospect"* (P2-III), they were quite keen to point out that in terms of prevention, most technologies would be simply futile:

> *"I do wonder also, what if someone who has been labelled as dangerous and you tag this person […] what happens if he does want to do something dangerous like within now and*

five minutes? Then tagging is not of much use, he has already done it anyways […] it has already happened" (P2-I).

Lastly, it appears that a number of participants also felt vulnerable since they perceived the misappropriation and misuse of personal data collected by smart surveillance and dataveillance as a very realistic and major threat; here the participants expressed their concerns that data "*can also be used by people for the wrong purposes"* (P7-III).

5.3.2 Perception of Different Technologies

In general, different types of surveillance technologies seemed to meet different levels of acceptance. While the use of video surveillance, sound sensors and Automatic Number Plate Recognition (ANPR) was on the whole considered as acceptable by the majority of participants, the use of biometric data and electronic tagging was, with few exceptions, considered as not acceptable.

The use of CCTV systems was considered not only as acceptable but also as necessary in certain locations, with very few participants objecting to the use of video surveillance. In relation to CCTV, some participants perceived the acceptance of this technology as possibly resulting from the normalization of surveillance:

"[…] with regard to CCTV, I've lived in England and America for a while and it was just much more extensive compared to here. And you do notice it at first but after a while you really get used to it and eventually I did kind of feel comfortable […] I did think it was a good feeling […] you just get used to it pretty soon" (P1-I)

On the other hand, the use of biometric data and electronic tagging – hence surveillance involving the physical sphere – was in general considered as *"quite radical"* (P8-II) and as extremely intrusive. In general, the collection of this type of data was perceived as presenting a higher threat to privacy: *"I think all these things violate your privacy to a certain extent"* (P5-I). Nevertheless, a few participants did appear to accept the use of biometric surveillance in specific cases such as the use of DNA for the investigation of violent crimes. Additionally, some also mentioned the benefits of biometric surveillance as in the case of biometric passports: *"Some people think that it is convenient that they easily let you through at Schiphol Airport"* (P8-II).

The use of electronic tagging brought about the strongest reactions amongst the participants: *"this tagging business really freaks me out"* (P8-II). While the participants strongly opposed the mandatory tagging of elderly people: *"I don't want it, imagine yourself on your 65th birthday nicely blowing out your candles and then they appear, 'hello, you have been tagged!'"* (P1-II), it appears that if electronic tagging was done on a voluntary basis it was then considered as acceptable, especially since the use of tagging could be life-saving in emergency situations.

With regards to locations of deployment, surveillance was considered as generally acceptable in public places, such as train stations, subways, city centers, museums and government institutions. Surveillance was also regarded as acceptable in private commercial establishments such as shopping centers. Moreover, several participants also indicated their acceptance of surveillance in sensitive areas such as airports and in areas considered as *"risk zones"* (P4-II):

> *"I think that's a good criterion, like risk areas, areas that have a lot of crime. It makes sense to introduce something there. In a garden where probably nothing ever happens it wouldn't make sense to put up cameras now, would it?" (P4-I)*

It appears that in general, surveillance in public places was considered as part of the 'caring' function of surveillance, and some pointed out that in this case, precedence should be given to the 'common good': *"I think you do have to consider sometimes what it is that provides the best safety for the largest group of people"* (P1-I).

On the other hand, surveillance was considered as unacceptable in private spaces such as one's home. Moreover, a number of participants from Group 1 (18-24 years) and Group 3 (45+ years) expressed their discomfort at being surveilled in the changing rooms of commercial establishments and public conveniences since participants perceived the latter as *"kind of private"* (P4-III).

5.4 Surveillance Laws & Regulations

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

5.4.1 A lack of information and transparency

During this part of the discussion, a lack of knowledge and initiative vis-à-vis the content of legislation was evident from the outset amongst some of the participants who for instance claimed *"I've never really looked into it"* (P8-III). Some participants from Group 1 (18-24 years) explained this lack of knowledge by arguing that legislation is *"rather vague"* (P3-I) for laypeople: *"Well I think it is too ambiguous, sometimes it is not immediately clear how things work with this privacy law and I think that is quite a problem*" (P1-I). Moreover, some participants from the same group proposed that information should be provided to citizens in a straightforward and transparent manner: *"[…] you just shouldn't need to investigate yourself in order to find out how things work. It just has to be clear"* (P3-I). While on the on hand some claimed that the onus should not be on the citizen, on the other hand others argued that the lack of initiative by citizens in getting informed about their privacy rights was a part of the problem: *"I think that if you really inquire about this, it will certainly become clear but I think that a lot of people are like, all these large chunks of text, never mind"* (P5-I).

5.4.2 Effectiveness of laws and regulations

Another issue discussed was the effectiveness of privacy laws. Participants' opinions were rather mixed in this regard; while some stated that they do feel protected by current legislation, several others expressed their misgivings regarding its effectiveness: *"I am under the impression that it is still kind of like a cheese full of holes"* (P6-III). Current legislation was thus perceived by some as requiring "*quite a lot of work"* (P8-II). It appears that a major reason why legislation was perceived as inadequate was the belief that laws are always a step behind the developments of the fast-moving technology:

> *"I think that when it comes to privacy legislation, because of developments in digital media, it's an area of law that is lagging behind. The law always lags behind, but in the area of privacy this is extreme" (P2-II)*

Nevertheless, others were keen to argue that it is *"inevitable"* that legislators will always be reactive: *[…] there's always a problem first and only then will you find a solution. So you need to have a problem first. Unfortunately that's a matter of cause and effect"* (P1-II).

5.4.3 Length of data storage

Participants were also asked about their opinions on the length of storage for surveillance data. Some participants considered this as a rather *"tricky question"* (P1-III) and expressed their hesitation in suggesting an appropriate storage period: *"It's very difficult for us lay persons to consider this"* (P8-II). Nevertheless, some did mention specific storage periods ranging between three and ten years as well as an indefinite length in relation to specific types of data.

In general, it appears that a number of criteria had a bearing on length of data storage, including purpose of use, type of data and locations under surveillance. Firstly, some participants argued that unless *"an incident"* (P3-III) happened, surveillance data should be disposed of immediately: *"[…] if there's no doubt that absolutely nothing happened then I think this information can be thrown away"* (P3-III). In contrast, others argued that surveillance data, even if no incidents are recorded, could be kept for a longer period for any possible use which may arise in the future.

Moreover, participants also distinguished between different kinds of data, arguing that storage length should be dependent on the type of data. Here the participants briefly discussed some types of data and suggested for instance that commercial data should have a maximum storage period of three years and that medical data should be kept indefinitely. In addition, it appears that participants generally favoured longer storage times for data related to *"criminal acts"* (P6-III). Participants argued that storage period should reflect the severity of the crime, distinguishing between petty crimes and more serious crimes.

Lastly, participants also differentiated between the storage of data from relatively low risk locations, such as commercial establishments, and the storage of data from locations considered as posing a *"higher risk"* (P4-I). In general, although no specific storage times were proposed in this regard, it seems that a longer storage period was considered as appropriate for surveillance data collected in sensitive locations such as airports.

6. Conclusion

Dutch participants displayed high awareness that individual citizens are indeed the subjects of surveillance in commercial, boundary and public spaces, as well as when making use of mobile devices. The results indicate that surveillance in these spaces has undergone a process of normalisation, and technologically-mediated surveillance is in these contexts regarded as mostly acceptable for security-related purposes as well as for marketing purposes in commercial spaces. Smart surveillance is perceived as more common in sensitive locations, such as airports and public places where mass events take place.

Most participants believed that massively integrated dataveillance is undoubtedly technically possible. However, they were of the opinion that legal restrictions and ethical concerns would prohibit the massive integration of personal data. A minority of participants believed that this practice is already taking place. Some of the Dutch participants believed that the possibility of dataveillance taking place also depends, in part, on individual behaviour as individuals should bear responsibility for divulging their personal information. Integrated dataveillance was generally considered unacceptable as it was believed to pose a threat to citizen privacy. It appears that acceptance was however contingent on several criteria including purpose of use, whether consent was provided, type of data to be collected and shared, and whether personal data was anonymised prior to being shared with third parties.

Views on the efficiency of smart technologies were rather polarised. While several participants regarded automatized surveillance systems as more efficient in comparison to those requiring a human operator, others were sceptical of technology on its own without human agency. A number of participants would prefer a surveillance process which includes a combination of technologically-mediated surveillance and the intervention of human operators.

An overwhelming majority of Dutch participants strongly questioned, upon reflection, the use of extensive surveillance for the sake of security, especially since they argued that security could never be fully guaranteed, even with the use of smart surveillance. While most participants acknowledged that the use of technology could be useful for purposes of investigation of crime, at the same time they expressed scepticism with regards to the use of surveillance technologies for the prevention of crime. Intrusive methods of surveillance were not only perceived as violating citizen privacy but also as providing a powerful tool to control citizens and to restrict individual freedom. Some participants also pointed out that extreme surveillance could possibly result in the general criminalisation of citizens. In light of this, most participants argued that extensive surveillance measures could not be justified even in case of escalating crime and correspondingly reiterated their refusal to sacrifice their privacy for the sake of security: "*I do believe that over the past hundred years or so they fought for how it is now, the situation as it is now, so I'd rather go for not having to sacrifice my privacy"* (P4-I).

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

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

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

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

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

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

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

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

- ☐ Yes
- ☐ No

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

- ☐ **Yes**
- ☐ **No**

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

- ☐ Yes
- ☐ No

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

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

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

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

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

- *Word-association game serving as an ice-breaker*
- *Establish top of mind associations with the key themes*
- *Start off the group discussion*

would like you to say the first couple of things that come to mind when you hear the word. Let's try an example first: What is the first thing that comes to mind if I say the word "*food*"? Preferably, try to think about single words or short phrases, avoiding lengthy descriptions.

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?

Aims:

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

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

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

4. Explore the participants' views on why their actions and behaviours are observed, monitored and collected

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

1. ***How is the information being collected:***

    a. ***Which types of technologies do you think are used to collect your personal information?***

2. ***What type of information is being collected:***

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

3. ***Who is collecting the information:***

    a. ***Who do you think is responsible for collecting and recording your personal information?***

    b. ***Where do you think your personal information will end up?***

4. ***Why 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...*

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

Aims
1. Participants' first reactions including:

Possibility / impossibility of scenario

Acceptability /

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

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

unacceptability of scenario

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

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

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

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

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?

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?

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)?

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

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

Running Total: 1 hour 15min

Reactions to scenarios

[About 20mins]

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

Item 5

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

Due to an significant increase in *violent crimes* in the capital city, including *a spate of kidnappings and murders which seem random and unconnected*, the state has decided to introduce CCTV surveillance in every public space, both those publicly owned (such as subways, public gardens and public conveniences) as well as those privately owned (such as shops, malls and taxis) which will enable automated face-recognition. In addition, all the cars passing through the main check points will have their number plates recorded. There are also plans to install sensors in all public areas which are able to detect loud

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

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

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

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

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

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

Aims:

1. Security climate and level of threat

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

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

2. Deployment of specific technologies

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

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

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

threat to your privacy? Why?

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

3. Locations of deployment such as:
Airports
Malls
Streets

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

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

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

4a. What do you think about privacy laws? Do they make you feel <u>protected</u>?

4b. Are there any <u>safeguards</u> or conditions that you would find <u>reassuring</u>?

5. Length of storage of surveillance data

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

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

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

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

Running Total: 1 hour 35min

Brief summary of discussion [5mins] ▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***Item 6 – Summing up session*** ***At the end of the focus group, it is helpful to provide a summary of the emerging points. Here you should aim at giving a brief summing up of the themes and issues raised during the discussion. After, you can ask for the following from the participants:*** - ***"How well does that capture what was said here today?"*** - ***"Is there anything we have missed?"*** - ***"Did we cover everything?"*** ***This brief session will give participants an additional opportunity to express their views and can also be used to elaborate on topics raised but not pursued at the time.*** ***Running Total: 1 hour 40 min***
Conclusion of focus group [5mins] ▪ ***Thank the participants*** ▪ ***Hand out the reimbursement*** ▪ ***Give information on SMART***	***Item 7 –Closure*** **With this last exercise our discussion has come to an end. May we take this opportunity to once again thank you for joining us and for sharing your opinions, experiences and thoughts.** ***At this point, hand out the reimbursements to the participants and inform the participants about the next steps.*** ***Give out more information about the SMART to the participants requesting such information.*** ***Total: 1 hour and 45 min***

APPENDIX C – DISCUSSION GUIDELINES (DUTCH)

Introductie	Instructie
Welkom participanten - *Verwelkomen deelnemers* - *Verstrekking van naamplaatjes* - *Tekenen van toestemmingsformulieren*	*Verwelkom de deelnemers als ze binnenkomen. Wijs hen een stoel en voorzie hen van een naamkaartje.* *Verdeel het toestemmingsformulier voor de deelnemers en vraag hen om dit te lezen en te ondertekenen voor de start van de focusgroep. Dit is van belang om te waarborgen zodat de deelnemers begrijpen wat zij zijn overeengekomen.*
Introductie [ongeveer 10 min] - *Bedanken* - *Introductie van het faciliterende team* - *Doel* - *Vertrouwelijkheid* - *Duur* - *Basisregels voor de groep* - *Korte introductie van de deelnemers*	**Welkom bij deze focus groep en bedankt dat u heeft ingestemd om te participeren tijdens deze sessie. Wij waarderen het dat U tijd genomen heeft ondanks uw drukke agenda om te participeren in dit project en uw betrokkenheid staat hoog in het vaandel.** **Mijn naam is _____ en ik zal de groepsdisuccie faciliteren. Ik word geassisteerd door _____ mijn collega, hij/zij zal aantekeningen maken en de discussie opnemen.** *Introduceer overige collega's als zij aanwezig zijn* **Onze sessie zal ongeveer anderhalf uur tot twee uur duren en omdat de discussie opgenomen wordt, vraag ik u allen vriendelijk om duidelijk te spreken; uw meningen en gedachten zijn erg belangrijk voor dit onderzoek, en we willen geen van jullie commentaren missen.** **Zoals vermeld toen u werd benaderd om te participeren tijdens deze discussie, gaat deze focus groep in op Technologie en Privacy, en het wordt uitgevoerd als onderdeel van het SMART Project, dat wordt medegefinancierd door de Europese Commissie. Voor degenen die meer willen weten over het SMART Project, laat het ons dan weten en wij zullen u meer informatie verschaffen aan het einde van de focus groep.** *In dit stadium is het belangrijk geen extra informatie te geven over de inhoud van de focusgroep om beïnvloeding en vertekening in de daaropvolgende discussie te vermijden.* **Zoals we u al hebben meegedeeld op het toestemmingsformulier wordt alles dat wordt opgenomen gedurende deze sessie vertrouwelijk behandeld en blijft uw identiteit anoniem.** **Dit betekent dat uw opmerkingen, nadat ze anoniem zijn gemaakt, alleen gedeeld worden door degenen die betrokken zijn bij dit onderzoek en gebruikt in wetenschappelijke publicaties met betrekking tot dit onderzoek. De informatie die wordt opgenomen in het rapport zal op geen enkele wijze naar u te herleiden zijn. Om dit te doen zal elke deelnemer een nummer krijgen. Dit getal wordt gebruikt in het verslag.** **Ik wil er ook voor zorgdragen dat iedereen in de groep zich zeker genoeg voelt om hun mening te delen. Om dit mogelijk te maken, wil ik alle aanwezigen vragen zich aan deze basisregels te houden.** **Wij willen van iedereen in de groep respons - We zijn geïnteresseerd**

	naar de mening van alle deelnemers. **Er zijn geen goede of foute antwoorden, dus respecteer de mening van anderen** **Zorg ervoor dat uw mobiele telefoons op stil staan zodat de discussie niet wordt gestoord.** **Aangezien de mening van iedere participant belangrijk is moeten alle deelnemers wachten tot de mededeelnemers uitgesproken zijn voordat ze beginnen met een opmerking. Laten we afspreken niet te spreken op hetzelfde moment, anders wordt het moeilijk voor ons om alles wat er wordt gezegd tijdens de discussie vast te leggen.** **Laten we elkaars vertrouwelijkheid respecteren zodat iedereen zich comfortabel voelt om openlijk te spreken.** **Als u een suggestie heeft voor een andere regel, voelt u zich dan vrij dit te melden aan de groep.** **Heeft iemand nog vragen voordat we beginnen?** **Ok laat ik beginnen met de vraag of u zich even kort voor kunt stellen aan de groep. Onthul hierbij geen prive-informatie. Laten we een ronde doen waarin u ons uw naam en misschien nog iets over u vertelt. Ik zal zelf beginnen...** *(Vertel de deelnemers een korte persoonlijke introductie).* *Tijdsduur: 10 min*
Objectives	**Discussion items and exercises**
Woordassociatie oefening **[ongeveer 5 minuten]** - *Woordassociatie-spel als een ijsbreker* - *Stel 'top of mind' associaties vast voor de belangrijkste thema's* - *Begin de groepsdiscussie*	***Item 1*** ***Eerst spelen we een klein spel. Ik lees een woord voor en ik zou graag willen dat u de eerste paar dingen zegt die te binnen schieten bij het horen van het woord. Een voorbeeld: Wat is het eerste dat in u opkomt ik het woord 'eten' zeg? Probeer lange beschrijvingen te vermijden en denk na over enkele woorden of korte zinnen.*** *Lees voor (één per keer):* *Technologie, privacy, nationale veiligheid, persoonlijke informatie, persoonlijke veiligheid* *Tijdsduur: 15min*
Discussie over alledaagse ervaringen met betrekking tot toezicht [20min] *-De ervaringen van deelnemers met bewaking nagaan en bekijken hoe zij dit beleven.*	***Item 2*** ***Laten we het ergens anders over hebben. Ik wil dat u nadenkt over gevallen waarin u het gevoel heeft dat uw acties worden geobserveerd of situaties waarin u zich ervan bewust bent dat er informatie over u wordt verzameld. We beginnen met activiteiten die u normaal gesproken zou ondernemen in uw dagelijks leven. De volgende situaties dienen als voorbeeld.*** **Scenario 1: Supermarkt** **Het eerste voorbeeld is een dagje winkelen bij uw gebruikelijke supermarkt. Wat zijn uw gedachten hierover?**

- De bewustzijn en kennis van deelnemers over verschillende surveillance technologieën verkennen.

Scenario 2: Reizen

Door met een andere situatie, dit keer met betrekking tot reizen. Hoe zit dat volgens u als u met het vliegtuig reist?

Scenario 3: Openbare ruimte (bijvoorbeeld een museum of een stadion)

Stelt u zich nu voor dat u een openbare plaats bezoekt zoals een museum of een evenement bijwoont zoals een sportwedstrijd of een concert. Welke activiteiten worden opgenomen denkt u?

Scenario 4: Mobiele apparaten

Laten we nu nog een laatste voorbeeld bediscussieren. Denk aan alle keren dat u uw mobiele telefoon gebruikt. Wat wordt er vastgelegd van uw gebruik?

Probeer voor elk onderdeel, en waar relevant, zo gedetailleerd mogelijk het volgende te achterhalen:

Doelen:

1. Aftasten van het bewustzijn en kennis van deelnemers van technologieen

2. Het verkennen van de ervaringen van deelnemers gecontroleerd te worden in hun verschillende rollen.,

3. Verkennen in hoeverre deelnemers begrijpen waar hun informatie eindigt.

4. Verkennen van de visie van deelnemers over waarom hun handelen en gedrag geobserveerd, gemonitord, en verzameld word.

1. ***Hoe wordt de informatie verzameld:***

   c. ***Welke technologieen worden er volgens u gebruikt om uw persoonlijke informatie te verzamelen?***

2. ***Wat voor informatie wordt er verzameld:***

   a. ***Wat voor persoonlijke informatie wordt er volgens u verzameld?***

3. ***Wie verzamelt de informatie:***

   a. ***Wie is er volgens u verantwoordelijk voor het verzamelen en vastleggen van uw persoonlijke informatie?***

   b. ***Waar komt uw persoonlijke informatie uiteindelijk terecht?***

4. ***Waarom wordt de informatie vastgelegd, verzameld en bewaard:***

   a. ***Waarom wordt uw persoonlijke informatie volgens u vastgelegd en verzameld?***

   b. ***Op wat voor manieren wordt uw persoonlijke informatie volgens u gebruikt?***

Tijdsduur: 35min

Presentatie van kaarten met beeltenissen van verschillende technologieen en toepassingen [10 minuten]

Deelnemers blootstellen aan een selectie van relevante smart-technologieen en toepassingen om ze deze beter te laten begrijpen en daarmee de discussie te vergemakkelijken.

Item 3

Presenteer de volgende drie kaarten (elk met een afbeelding van een groep verschillende technologieen en toepassingen) aan de groep. De kaarten tonen de volgende afbeeldingen:

***Kaart 1 – Herkenning van personen of gebeurtenissen en tracking technologieen**: Automatische bewegingsregistratie met cameratoezicht of -bewaking (CCTV – Closed Circuit Television); Automatische kentekenplaatherkenning (ANPR) of automatische voertuignummerherkenning (AVNI); en tracking apparatuur zoals mobiele telefoon en RFI.*

***Kaart 2 - Biometrie**: Biometrische technologieen met onder meer vingerafdrukken en irisscans, en automatische gezichtsherkenning (AFR)*

***Card 3 – Object- en product-detectieapparatuur**: Veiligheidspoortjes en Rontgenapparatuur*

Tijdsduur: 40min

Presentatie van MIMSI scenario aan de deelnemers

[30minuten]

- *Het verkennen van het begrip en implicaties van MIMSI bij de deelnemers*

- *Het verkennen van de gevoelens, overtuigingen en houdingen van participanten ten opzichte van het delen van persoonlijke informatie.*

- *Het verkennen van de gevoelens, overtuigingen en houdingen van participanten ten opzichte van het delen van persoonlijke informatie.*

Item 4

Presenteer het onderstaande hypothetische scenario aan de groep. Een opname van de telefonische conversatie kan vooraf worden voorbereid en voorgelegd aan de groep.

Telefoon conversatie met een medewerker van de klantenservice van de belangrijkste tak bij de Openbare Dienst voor Arbeidsvoorziening

Klantenservice: Goedemorgen u spreekt met Sharon, hoe gaat het met u meneer Brown? We hadden uw oproep reeds verwacht nadat uw arbeidscontract meer dan een maand geleden is geeindigd.
Mr. Brown: Erm...ja dat is in feite ook de reden waarom ik bel…
Klantenservice: Nou, ik ben eigenlijk niet verbaasd dat je nu belt… Hoe was je vakantie in Cyprus? Ik ben er zeker van dat je vrouw en kinderen genoten van het resort waarin jullie verbleven…
Mr. Brown: Ja het was een heerlijke vakantie … en hoe weet je dit allemaal?
Klantenservice: Het staat in het systeem, meneer Brown … kennelijk. Hoe dan ook, beter een voorsprong op het vinden van een nieuwe baan … want met de kosten van uw vakantie met het hele gezin en met de betaling van uw auto in het vooruitzicht … en niet te vergeten uw VISA betaling op de 22e van deze maand …
Mr. Brown: Staat dit ook in uw systeem?
Klantenservice: Ja, natuurlijk meneer Brown. Overigens, goede keuze voor dat boek dat u online gekocht heeft… Ik lees het zelf en het gaf me een paar goede tips…
Mr. Brown: Hmmm...ok...met betrekking tot deze nieuwe werkzoende dienst, is het nodig om een geupdate foto van mezelf te geven?
Klantenservice: Nee meneer Brown, daar is al voor gezorgd, natuurlijk! We hebben genoeg recente foto's in ons systeem. Dat herinnert me aan… heerlijke zonnebrand hadden jullie bij je op vakantie! Het moet vast prachtig weer zijn geweest! Voordat ik het vergeet, met betrekking tot de foto, geeft u de voorkeur aan een foto met uw bril op of een zonder?
Mr. Brown: Oh...nou....zonder is prima...even over mijn registratie, kunnen we een afspraak maken, ergens volgende week?
Klantenservice: Ik check even het systeem… hoe zit u woensdagmiddag? Oh wacht eens even! Ik zie net dat je een afspraak met de dokter gepland hebt staan op dat moment. En ik weet zeker dat je die niet wilt missen, omdat de controle van uw cholesterolgehalte zeker belangrijk is! Wat dacht u van een afspraak op donderdag om negen uur 's morgens?
Mr. Brown: Donderdagmorgen is prima… moet ik wat documenten meenemen?
Klantenservice: Nee meneer Brown, we hebben al alle informatie die we nodig hebben in ons systeem.
Mr. Brown: Ik ben er zeker van...
Klantenservice: Bedankt voor het bellen meneer Brown en tot volgende week. Overigens, geniet van uw cappuccino bij Cafe Ole'...
Mr. Brown: Ik ben … tot ziens...

Na de presentatie van het vorige scenario aan de groep, probeer meer de diepte in te gaan door het volgende te ontdekken:

Doelen

1. De eerste reacties van de deelnemers inbegrepen: Mogelijkheid / onmogelijkheid van

1a. Hoe zou jij je voelen als dit bij jou zou gebeuren?
(Peil ook de mate van controle / hulploosheid die opkwam bij de participanten in een dergelijk hypothetisch scenario)

1b. Hoe zou jij reageren als dit met jou gebeurd? Wat zou je doen?

scenario Acceptabel / onacceptabel scenario

2. overtuigingen en houdingen over hoe technologie invloed heeft of invloed zou kunnen hebben op hun privacy

3. Overtuigingen en houdingen van deelnemers ten aanzien van de aard van de informatie, zoals: Medische dossiers; financiële informatie; foto's en locatie.

4. Overtuigingen en houdingen van deelnemers op het verzamelen, het gebruik en het delen van persoonlijke informatie met derden.

5. Overtuigingen en houdingen van participanten over de voor- en nadelen van het registreren van acties en gedrag.

1c. Is een dergelijk scenario mogelijk / onmogelijk?

1d. Is een dergelijk scenario acceptabel / onacceptabel?

2a. In welke mate denkt u dat "stand alone" (individuele technologieën) invloed hebben op uw privacy?

2b. In welke mate denkt u dat "smart-technologieën", dwz welke gegevens verwerken in een geautomatiseerd (of semi-automatische) manier invloed hebben op uw privacy?

3a. Wat voor soort persoonlijke informatie vindt u aanvaardbaar om verzameld, gebruikt en / of gedeeld te worden?

3b. Wat voor soort persoonlijke informatie zou u bezwaar tegen maken als het wordt verzameld, gebruikt en / of gedeeld?

4a. Wat vindt u ervan dat uw persoonlijke gegevens worden verzameld, gebruikt en gedeeld door de staat?

4b. Wat vindt u ervan dat uw persoonlijke gegevens worden verzameld, gebruikt en gedeeld door particuliere entiteiten (zoals commerciële alternatieven)?

5a. Denk je dat er voordelen zijn aan het registreren van uw acties en gedrag?

5b. Denk je dat er nadelen kleven aan het registreren van uw acties en gedrag?

Tijdsduur: 1 uur 15min

Reacties op scenarios

[Ongeveer 20 minuten]

-Om een debat te stimuleren, om de perceptie van de deelnemers met betrekking tot "veiligheid versus privacy" te verkennen.

- Hier moet de discussie zich niet richten op de vraag of deze technologieën de veiligheid zullen verhogen
- Dit moet beschouwd worden als een gegeven. De discussie moet vooral gaan over het feit of deze technologieën effect hebben op privacy en daarom draaien rondom de afweging wel / geen privacy.

Item 5

Tijdens de volgende oefening bespreken we het volgende hypothetische scenario. Stel je het volgende voor:

Als gevolg van een significante toename van geweldsdelicten in de hoofdstad, met inbegrip van een golf van ontvoeringen en moorden welke random lijken en met geen verband, heeft de staat besloten om cameratoezicht (CCTV surveillance) te introduceren in elke openbare ruimte, zowel de publiekelijke (zoals metro's, openbare tuinen en openbare toiletten) evenals die in particulier bezit (zoals winkels, winkelcentra en taxi's), waarmee geautomatiseerde gezichtsherkenning toegepast kan worden.
Daarnaast wordt van alle auto's die door de belangrijkste controlepunten rijden, hun kenteken geregistreerd. Er zijn ook plannen om sensoren te installeren in alle openbare ruimten die in staat zijn om harde geluiden op te sporen, zoals het geval is als iemand schreeuwt. Alle burgers zullen worden verplicht om hun DNA en vingerafdrukken af te staan, en hun iris wordt gescand. De staat heeft ook besloten dat alle burgers die een mogelijk risico vormen voor anderen, elektronisch gelabeld moeten worden zodat ze kunnen worden gecontroleerd en hun bewegingen gevolgd kunnen worden. Voor hun veiligheid zullen ouderen en kinderen tot 12 jaar ook elektronisch gelabeld worden. Alle gegevens afkomstig van deze verschillende technologieën zullen worden opgeslagen in gekoppelde databanken beheerd door de politie, die automatisch een melding krijgt als er een reden is voor alarm en risico voor iedere burger.

.....

Variant 1: Ook al vindt er een aanzienlijke toename plaats van gewelddadige criminaliteit in het merendeel van de omliggende steden, de stad waar jij woont heeft geen last van een toename van criminaliteit. Echter, de staat beslist toch om de maatregelen van toezicht in te voeren als een voorzorgsmaatregel.

.....

Variant 2: In het algemeen heeft het hele land een weinig criminaliteit, maar de staat besluit toch om toezicht maatregelen uit voorzorg in te voeren nadat in een naburige stad een incident heeft plaatsgevonden waarbij een aantal mensen werden neergeschoten en ernstig gewond raakten door een man die het vuur opende in een winkelcentrum.

Tijdens de bespreking van het bovenstaande scenario en de variaties, tracht om in detail de volgende factoren te onderzoeken en hoe deze de vraag rondom wel / geen privacy van invloed zijn:

Doelen:

1. Veiligheidsklimaat en mate van dreiging

1a. Wat geeft u een <u>veilig</u> gevoel in het gegeven scenario?

1b. Wat geeft u het gevoel <u>kwetsbaar</u> zijn in de daarvoor bestemde scenario?

1c. Zou u bereid zijn om uw privacy op te offeren als het niveau van de dreiging anders was als in variant 1 en 2 van het scenario?

2. Inzet van specifieke technologieen

2. Van de slimme technologieën uit het scenario, dat wil zeggen:

CCTV met Automatische Gezichtsherkenning
Automatische Nummerbord Herkenning (ANPR),
Sensors (met de mogelijkheid om harde geluiden te detecteren),
Biometrische technologieen (inclusief fingerprinting) and
Electronisch tagging (waarbij RFID gebruikt wordt)

2a. Welke technologieen vindt u <u>acceptabel?</u> Waarom?

2b. Welke technologieën zijn een inbreuk maken op en ziet u als een bedreiging voor uw privacy? Waarom?

2c. Wat vindt u van deze geautomatiseerde (of semi-automatische) technologieën waarbij de uiteindelijke beslissing wordt genomen door het systeem en niet door een menselijke operator?

3. Locaties van de inzet, zoals: luchthavens winkelcentra straten

3a. Welke locaties vindt u <u>acceptabel</u> om geregistreerd te worden? Waarom?

3b. Welke locaties vindt u onacceptabel om geregistreerd te worden?

4. Bestaan van wetten en andere waarborgen (met betrekking tot het verzamelen, opslaan en gebruiken van gegevens)

4a. Wat vindt u van privacy wetgeving? Zorgt het ervoor dat u zich <u>beschermd</u> voelt?

4b. Zijn er <u>garanties</u> of voorwaarden die u <u>geruststellend</u> vindt?

5. Lengte van opslag van toezichts gegevens.

5a. Wat vindt u van de lengte van opslag van de toezichtsgegevens? Maakt het een verschil?
Om te helpen om dieper te gaan, verstrek de volgende voorbeelden aan de participanten:

- ***Opnames van CCTV***
- ***De locatie en bewegingen van auto's***
- ***De opslag van DNA, vingerafdrukken en iris scans***
- ***De locatie van burgers die een risico vormen voor anderen***
- ***De locatie en bewegingen van ouderen en kinderen***

5b. Als de duur van opslag een verschil zou maken, wat zou je beschouwen als een <u>aanvaardbare termijn</u>?

Tijdsduur: 1 uur 35min

Doelstellingen	Samenvattende sessie
Korte samenvattingen van de discussie [5 minuten] ▪ *Bevestig de belangrijkste aangedragen punten* ▪ *Schep een verdere kans om te werken aan wat er tot nog toe is gezegd*	***Item 6*** ***Aan het eind van de focusgroep is het behulpzaam om een overzicht te geven van naar voren gekomen punten. Mik hierbij op het geven van een korte samenvatting van de thema's en problemen die naar boven zijn gekomen tijdens de discussie. Naderhand kun je de deelnemers het volgende vragen:*** - **"Hoe goed geeft dit weer wat er vandaagd is gezegd?'** - **"Is er iets dat we hebben gemist?'** - **"Hebben we alles behandeld?"** ***Deze korte sessie geeft de deelnemers een extra mogelijkheid om hun denkbeelden te uiten en kan ook gebruikt worden om onderwerpen uit te werken die wel aan bod zijn gekomen, maar waar niet dieper op in is gegaan.*** ***Tijdsduur: 1 uur 40 minuten***

Doelstellingen	Sluiting
Afronden van focusgroep **[5 minuten]** ▪ ***Bedankt de deelnemers*** ▪ ***Reik de vergoeding uit*** ▪ ***Geef informatie over SMART***	***Item 7*** **Met deze laatste oefening is onze discussie tot een eind gekomen. Mogen we deze mogelijkheid aangrijpen om u opnieuw te bedanken voor het deelnemen en het delen van uw meningen, ervaringen en gedachten.** ***Nu is het moment om de vergoeding uit te reiken aan de deelnemers en leg ze uit wat de vervolgstappen zijn.*** ***Geef meer informatie over SMART aan deelnemers die daar benieuwd naar zijn en naar vragen.*** ***Totale Tijdsduur: 1 hour 45 min***

APPENDIX D – DEBRIEFING FORM

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

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

APPENDIX E – CONSENT FORM

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

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

1.1. Commercial space

1.1.1. Awareness of different surveillance methods/technologies

1.1.1.1. CCTV

1.1.1.2. Loyalty cards

1.1.1.3. Financial monitoring

1.1.2. Perceived purposes

1.1.2.1. Security purposes

1.1.2.2. Commercial reasons

1.2. Boundary (border) space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. CCTV

1.2.1.2. Smart CCTV with AFR

1.2.1.3. Biometric technologies

1.2.1.3.1. Fingerprinting

1.2.1.3.2. Retinal scanning

1.2.1.3.3. Iris scanning

1.2.1.4. Object and product detection devices

1.2.1.4.1. Luggage controls

1.2.1.4.2. Body scanners

1.2.1.4.3. Metal detectors

1.2.1.5. Monitoring of personal data

1.2.1.5.1. Passport control

1.2.1.5.2. Passenger lists

1.2.1.5.3. Airline booking system

1.2.1.6. Security staff

1.2.1.7. Sniffer dogs

1.2.2. Perceived purposes

1.2.2.1. National security

1.2.2.2. Traveller safety

1.2.2.3. Commercial motivations

1.2.2.4. Collection of statistics

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV

1.3.1.2. Television cameras

1.3.1.3. Audio-equipment

1.3.1.4. Collection of personal data
1.3.1.5. Security officers
1.3.1.6. Law enforcement personnel
1.3.2. Perceived purposes
1.3.2.1. Public security
1.3.2.1.1. Timely identification of trouble-makers
1.3.2.1.2. Investigation of incidents
1.3.2.2. Citizen safety

1.4. Mobile devices and virtual spaces
1.4.1. Awareness of different surveillance methods/technologies
1.4.1.1. Location tracking via GPS
1.4.1.2. Monitoring of call lists
1.4.1.3. Recording of conversations (wiretapping)
1.4.1.4. Collection of data through smart phone applications
1.4.2. Perceived purposes
1.4.2.1. Commercial purposes
1.4.2.2. Generation of statistics
1.4.2.3. Security-related functions

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

2.2. Behavioural intentions
2.2.1. Passive reactions
2.2.1.1. Immediate withdrawal

2.2.2. Self-protection strategies
2.2.2.1. Investigate
2.2.3. Establish lobby group

2.3. Beliefs
2.3.1. Likelihood of smart surveillance and dataveillance
2.3.1.1. Technical aspect
2.3.1.1.1. Possible due to integration of data
2.3.1.1.2. Self-responsibility

2.3.1.2. Legal aspect
2.3.1.2.1. Legal restrictions
2.3.1.3. Ethical aspect
2.3.1.3.1. Invasion of privacy
2.3.2. Acceptance of dataveillance
2.3.2.1. Purpose of use
2.3.2.2. Anonymisation of data
2.3.2.3. Consent
2.3.2.4. Access to data
2.3.2.4.1. State
2.3.2.4.2. Private entities
2.3.2.5. Type of data stored and shared
2.3.3. Perceived effectiveness of smart technologies
2.3.3.1. Decision-making capabilities of automated systems
2.3.3.2. Human agency

3. Security-privacy trade-offs

3.1. Acceptance of technological surveillance
3.1.1. Feelings
3.1.1.1. Vulnerability and insecurity
3.1.1.2. Safety
3.1.2. General beliefs
3.1.2.1. Extreme form of control: association with a totalitarian regime
3.1.2.2. Observation of citizens: criminalisation of citizens
3.1.2.3. Violation of privacy and freedom
3.1.2.4. Safety and peace of mind: the “caring” function of surveillance
3.1.3. Effectiveness of surveillance
3.1.3.1. Ineffectiveness in offering protection and prevention
3.1.3.2. Effective for investigation purposes
3.2. Perceptions of different technologies
3.2.1. CCTV
3.2.2. Biometric data and electronic tagging (RFID)
3.2.2.1. Strong perceptions of bodily/physical invasiveness
3.2.2.2. Sense of discomfort and uneasiness
3.2.2.3. Treat to freedom

3.3. Locations of deployment
3.3.1. Acceptable: the ‘caring function’ of surveillance
3.3.1.1. Public places
3.3.1.2. High risk areas
3.3.2. Unacceptable

3.3.2.1. Private spaces and private spheres

4. Surveillance laws and regulations

4.1. Feelings and beliefs

4.1.1. Knowledge and awareness of legislation

4.1.2. Effectiveness of laws and regulations

4.1.3. Length of data storage