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

Noellie Brockdorff[1], Sandra Appleby-Arnold[1], Christine Garzia[1], Rozemarijn van der Hilst[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Norwegian Data Protection Authority, Oslo, Norway

April 2014

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

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

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

Table of Contents

1. Key Findings

This document presents the Norway 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 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, 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 Norwegian participants revealed a general awareness that, as citizens, they are subjected to surveillance in different contexts. In commercial spaces, their perceptions ranged from strong awareness to acceptance and adaptation, with surveillance via bank and loyalty card raising increased feelings of discomfort. In the context of border control where they also felt under comprehensive surveillance, the merging of biometric and behavioural data appeared to cause particular unease. In common public spaces and, in particular virtual spaces, participants revealed their suspicions about potential reuse or misuse of their personal data which, in the latter case, was strongly related to their extensive technical knowledge about the functionalities of online social networks.

In order to gauge participants' attitudes on the massive integration of data, the groups were presented with a fictional scenario illustrating the occurrence of complex surveillance, After indicating an extreme sense of discomfort, the participants' behavioural intentions ranged, here, from retreat into an "inner world" to active protest. The majority, however, revealed a strong perceived helplessness – or denial.

Despite apparent difficulties to imagine the possible extent and complexity of surveillance measures, most of the participants agreed that such practice would be not acceptable to them. Here, their primary concern was not only that an increasing complexity of such systems would bear the increased risk of unauthorised access, but also that the more data was collected over an extended period of time, the more likely it would be that the collected pool of data contained something that may be used against the respective individual. This points to data security not being a mere problem of "interior" safety (i.e. storage systems or access rules), but also subject to "exterior" factors such as complexity and time.

With regards to the conceptualisation, and effectiveness, of technological surveillance, it appeared that most participants predominantly focussed on the automatic decision-making process of smart technologies, which brought up mixed feelings and beliefs: some revealed a certain trust in technology itself, although others believed that any technological solution would always be limited because of its tendency to result in "black-or-white decisions" which was seen to be against human reality. In contrast,

stand-alone “traditional” surveillance techniques based on human decision were seen to potentially carry the problem that, due to human error, important information may not only be intentionally dismissed but, simply, accidentally missed out. However, as one of the main difficulties with putatively “smart” surveillance technologies it was highlighted that any technology would be based in its automated decision-making on human experience and, therefore, lack the ability to learn genuinely new things as well as human intuition.

Regarding the general acceptance of technological surveillance, it was felt that indiscriminate data collection in combination with smart technologies would violate basic human rights by marking every citizen as a “potential risk” without good cause. However, privacy appeared not to be perceived as something that was either strongly violated or to be traded in this context. As specific technologies, CCTV cameras and ANPR seemed to be more accepted, whilst biometrical surveillance, if used for screening entire populations, was perceived as the most invasive technology. Geolocation tracking was seen to be particularly problematic if used with vulnerable groups such as elderly or children, because those were seen to be potentially incapable of giving fully informed consent to such tracking.

Beliefs around the effectiveness of surveillance laws and regulations varied considerably according to age. Younger participants did not feel sufficiently protected by current legislation, whilst some older participants showed a rather strong trust in the effectiveness of Norwegian privacy laws and the Norwegian Data Protection Authority as not only protecting the mere data but also citizens’ interests.

Ultimately, the Norwegian participants’ main concerns in the context of personal data collection (from surveillance or otherwise) on a massive scale and in combination with long-term storage appeared to be twofold: They did perceive generally increased data security issues, but what appeared to worry them more was the gradual build-up of a complex data-based “digital collective memory” which may not be as merciful and forgiving as human memory. Their trust in the Norwegian state as a welfare-oriented social institution seemed partially to be shaken by perceptions that control – rather than care – was increasingly becoming of primary interest to public authorities. This could be interpreted as evidence that trust in the government is grounded in a government’s personal care for its citizens, i.e. people being there for people – and that such care can be substituted by surveillance technologies only to a limited extent.

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, and coordination between partners, data analysis and report writing. The SMART project partners in each country were responsible for the translation and back-translation of the research materials, recruitment of participants, recruitment and briefing of moderators, conducting the focus groups, transcription of the discussions, and translation of transcripts into English. The SMART project partner for Norway is the Norwegian Research Centre for Computers and Law at the University of Oslo.

Focus group discussions were conducted in a total of 14 countries and this document provides the findings from the study that are relevant to Norway. Other separate reports are available for Austria, Bulgaria, Czech Republic, France, Germany, Italy, Malta, the Netherlands, 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	5	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	**121**		**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, 352 participants took part in this research project. The focus groups in Norway were carried out on the 3rd, 4th, and 11th of June 2013. It should be noted that between the 4th and 11th of June, 2013, the revelations made by Edward Snowden with regards to the mass surveillance programmes undertaken by the National Security Agency (NSA) came to light in the media. Although these revelations were not mentioned during the Group 3 (45+ years) discussion, the disclosures about government surveillance might have nevertheless influenced the views of the participants in this group. The composition of the groups held in Norway 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 Norwegian 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

4.1 General Description

The data analysis for Norway 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	M	F	F
P2	F	M	M
P3	M	M	F
P4	F	F	F
P5	M	M	M
P6	F	F	F
P7	F	M	F
P8	F	-	-
Total	**8**	**7**	**7**

In general, the atmosphere of the first group (18-24 years) was described by the moderators as slightly awkward, the participants being not very engaged and appearing slightly shy, over-polite and rather unhappy with any disagreement between each other. The slow-going discussion was ascribed by the moderators partially to the participants' young age and, partially, to a low familiarity with some of the surveillance technologies in question.

The atmosphere in groups 2 (25-44) and 3 (45+) appeared to be rather different, participants being very engaged and interested. The discussions were described by the moderators as smoothly flowing, and in both groups the participants appeared happy to discuss controversial viewpoints between each other. In particular the discussion between participants of group 2 was described as enthusiastic, trustful, and intense.

4.2 A Note on Gender Differences

Generally, it appeared that female participants expressed their emotions (which were more often negative than positive) more frequently, whereas male participants tended to focus more on awareness and "technical" aspects such as practicality or data safety. It is, hence, tempting to interpret this as female citizens actually feeling more affected by surveillance – and, due to the higher frequency of negative emotions, feeling more exploited, violated, and insecure.

However, when being probed directly about their feelings, male and female participants showed very similar reactions, which allows for the assumption that such higher frequency of expressed emotions cannot easily be equated with stronger emotions. Instead, the noted differences may be more related to gender-specific cultural preconditions such as education and strategies in self-expression, rather than gender-specific feelings and perceptions of surveillance. For a more grounded analysis of potential

gender differences in feelings and perceptions of surveillance, a research design would be required that takes into consideration – and probes – these particular effects.

5.1 Surveillance Technologies in Different Spaces

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

5.1.1 Commercial Space

In commercial spaces, participants of all ages mostly perceived video-surveillance systems and the use of bank or loyalty cards as the predominant methods through which consumers are monitored. Particularly CCTV monitoring was felt to be very comprehensive:

> *"When you buy something. As soon as you enter the store, there is a camera on you. And throughout the entire store, from entrance to exit, so you by and large have a camera on you continuously. The only exceptions are in the office, and in the dressing rooms and toilets. Otherwise it is pretty much full monitoring"* (P7-II).

Whereas the younger participants (group 1), generally, did not reveal any feelings of discomfort about these types of surveillance, participants in the other two groups expressed perceptions that were ranging from strong awareness – *"I think quite often about it when I buy things: that I am actually monitored"* (P3-II) – to acceptance and adaptation: *"I know there are cameras, but I must admit I very rarely think that I'm being observed"* (P4-III). At the same time, some participants outlined as a positive aspect that CCTV monitoring was not covert surveillance, but *"the first thing you see when you come in is a monitor, where they show that you are being filmed"* (P6-II).

In contrast, bank and loyalty cards appeared to raise more feelings of discomfort: *"I often think that they know what I have bought, and where, when I pay by card, and I can feel a bit uncomfortable"* (P3-III). Such discomfort was specifically ascribed to this form of surveillance as being not connected to a particular location (which could, perhaps, be avoided), but "following" the individual around: *"I think about it more when I swipe my card [...] As long as I have a card I can be traced as long as I am using it – on trips, or when I buy things, or anywhere at all"* (P5-II).

Regarding the perceived purpose of surveillance in commercial spaces, particularly the younger focus group participants appeared to accept that it is used for marketing purposes as well as the prevention or prosecution of theft, the latter reason also mentioned by the older participants. One participant tentatively linked the usage of data from surveillance in commercial spaces to another level:

> *"I just think: We focus on the shop and consumer habits and, of course, banks also monitor their customers when using a bank card – they also look at user habits. But in addition to this*

there is a third thing I'd like to point out, and maybe it is only me who thinks this, but if you find yourself in an unfortunate situation, the police can also monitor your movements in relation to bank cards. So there are several levels here" (P3-III).

However, this topic of a "layered' surveillance, i.e. that surveillance data related to commercial spaces may be used by a variety of different individuals or institutions, was not taken up at that point in the discussion by any of the other participants, but it was rather linked back to the prevention and prosecution of fraud.

5.1.2 Boundary Space

In the context of border control, the discussion mainly focused on an airport setting as a boundary space. Surveillance, there, was considered as ubiquitous, and focus group participants in all groups showed a strong awareness that *"everything"* (P4-I) was registered: from ticket purchase where personal and travel-related data are linked to bank card data, biometric data in passports, to behavioural data gathered through tax free shopping. Particularly the merging of biometric and behavioural data appeared to cause certain unease:

"There is an insane amount of information in my passport. It is also quite electronic now, so they certainly see everywhere I have travelled before and where I have utilised it. As well as how tall I am, what I look like – the entire package" (P5-II)

Regarding the question of who is using these data, predominantly participants of group 1 (18-24 years) outlined reasons beyond national security, namely *"business intelligence"* (P1-I), i.e. marketing purposes and business strategies. Otherwise, most participants agreed that it was *"the state first and foremost"* (P5-I), and they showed a certain awareness that data between airlines and national security forces would be shared, as well as between national and transnational authorities (e.g. Europol). However, massively integrated and smart surveillance systems were not explicitly mentioned in this context.

Another reason mentioned for such surveillance in this boundary space that goes beyond security was *"fear reduction"* (P6-II) – though perceived as *"extremely ineffective"* and being *"there in order for people to believe that there is someone who is in control: 'It is not dangerous to fly'"* (P6-II). Additionally, participants of group 3 (45+ years) speculated that data collected through surveillance in boundary space may also be used for purposes other than border control: "*What is a problem is that it is exploited, and who sets the criteria for using and not using the information"* (P3-III). However, it appeared to be a discomfort that was not strong enough to result in behavioural consequences: "*Unfortunately, you cannot avoid this if you buy a plane ticket online"* (P3-III).

5.1.3 Common Public Spaces

In common public spaces, such as town squares, exhibitions, or stadiums where mass events like concerts are organised, participants predominantly mentioned two methods through which, in their opinion, surveillance occurs: CCTV cameras – either for protecting *"highly valuable things"* (P5-II), e.g. in museums, or for crowd control, e.g. in football games. The latter, however, was believed to be mostly taken care of by *"large guards in yellow or green vests [...] They look for known people, who they often have seen pictures of as a point of departure, and who they look for at the entrance"* (P1-II).

The form of surveillance more often mentioned by participants in all groups was the monitoring of data collected through ticket purchase. Whereas participants in group 1 (18-24 years) perceived such surveillance as solely being used for marketing, or for preventing fraud, participants of the two other groups mostly outlined security reasons. Here, one participant described how she started noticing that admission tickets had changed: *"Before, when I went to festivals, I had a completely simple ticket, but now in recent years my name is always on the ticket"* (P4-II). This comment initiated a discussion in group 2 (25-44 years) around who would make use of these data and why it was collected: Whereas some participants developed the idea that *"the PST [Norwegian Security Service] certainly collects everything at the trailing edge [... and] everything goes further up to the end"* (P2-II), others rejected this idea, believing that *"when it is private companies, then they do not have contact with the PST in that manner. And the PST is not authorised to monitor private companies in that manner"* (P4-II). Such institutional adherence to (assumed) data protection rules, however, remained questioned – *"But are we sure that they do not do it anyway? Can we be sure? [...] Who knows how far they actually are – perhaps they are just better at hiding it"* (P7-II). Here, the participants exposed a critical underlying awareness which, perhaps, emerges only when citizens are given the opportunity for joint reflection.

5.1.4 Mobile Devices and Virtual Spaces

Participants from all age groups appeared to be aware of surveillance when making use of a mobile device. They revealed a belief that data such as who is calling, call duration, and from/to where the call is made, were gathered by telephone companies because *"they have to"* (P5-I) and that, for security reasons, they are legally obliged to store these data. Additionally, in particular group 1 participants (18-24 years) appeared to be aware of and accepted geolocation tracking by police or security forces as a measure to prevent or prosecute crime. Most participants also agreed that *"if I have a desire to be invisible, then I must switch off my telephones"* (P7-II).

Regarding surveillance of virtual spaces in general, the majority of participants revealed a broad knowledge about the functionalities of online social networks and the data collected there. Data protection in this area was believed to be rather limited – either due to fraudulent hacking, but also because of public authorities collecting data without the required permission: *"There is quite a lot that is stored that even the police does not have authorisation to see – but then they find a way to see it anyway"* (P2-II). Ultimately, some participants expressed their opinion that everyone should bear his share of responsibility for data security:

"We can certainly blame ourselves, but we can also blame Facebook, and we can also blame those who have done such things that the rules can be abused by Facebook. And, then, it is of course the authorities who are responsible when all is said and done" (P7-II)

Such (self-)critical statements, alongside the participants' extensive knowledge about data monitoring in virtual spaces, may be interpreted as an effect the public discussions about online privacy have had on awareness of surveillance in online social networks. This would be confirmed by the observation that group 3 participants (45+ years) also revealed a rather detailed knowledge of using mobile and smart phones for online social networking, but did not mention geolocation tracking at all.

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, they 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. Group 1 participants (18-24 years) described themselves as "*persecuted*" (P8-I) or "*frightened*" (P7-I), the latter for two specific reasons: due to the uncertainty of how the personal information was gathered, and a perceived lack of control regarding any further information transfer. Participants of group 2 (25-44 years) felt *"alarmed"* (P5-II), particularly *"annoyed"* (P3-II, P5-II), *"furious"* (P7-II), *"shocked"* (P6-II), *"violated"* (P1-II), or at least *"a bit disheartened"* (P2-II). Participants of group 3 (45+ years), however, revealed very little emotions – only one stated that *"I think I would have felt quite paranoid"* (P1-III). All others in this group immediately started to rationalise the situation as *"an example of something that should not happen and, perhaps, does not happen either"* (P4-III).

5.2.2 Behavioural Intentions

In addition to asking about their feelings upon listening to this conversation, participants were asked for their resulting behavioural intentions, which varied between the different age groups. Group 1 participants (18-24 years), despite feeling "persecuted" or "frightened" (see quotes above), described how they would try to take action and refuse or delimit access to their personal data. Similarly, some participants in group 2 (25-44 years) stated that they *"would have started a demonstration"* (P7-II), showing a rather active reaction. The majority of participants in this age group, however, suggested more passive behaviours, revealing a strong perceived helplessness, a possible retreat into an "inner world", and paranoia:

> *"I believe I would have become quite paranoid, because if I had had a desire to do something about it, I would of course have found out that they knew whatever I was doing, where I was going and who I was talking to. So how could you then be able to do anything about it?" (P5-II).*

[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.

Participants of group 3 (45+ years), finally, did not express any strong behavioural intentions, but immediately started talking about their beliefs – a behaviour which could be interpreted as acceptance, but also as denial.

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 were possible (currently or in the future), it appeared that a considerable number of participants had difficulties to imagine such extent and complexity of surveillance. However, during the discussions, a reflection process started where the rejection of the scenario by the participants as hypothetical and unreal turned gradually into critical rethinking: *"There is actually something to it"* (P3-II). Only participants of group 1 (18-24 years) appeared to have little problems to at least "play" with the idea of the presented scenario being possible. Distinguishing between technical and legal aspects, they either expressed their belief that it would, technically, not be possible because *"it requires an immense amount of resources"* (P5-I), or they felt that *"it's possible, but not legal"* (P4-I).

5.2.3.2 Acceptance of smart surveillance and integrated dataveillance

After discussing the likelihood of massively integrated dataveillance, the participants also discussed the topic of (non-)acceptance, most of them agreeing that such practice would be *"totally unacceptable"* (P7-II). However, given their aforementioned difficulties to comprehend the concept of such surveillance, it appeared that they "translated" it for themselves into issues with data security rather than with the collection of data: *"It is certainly the aspect about storage I actually struggle with the most. Things are stored there which I cannot trust they're being kept safely"* (P5-II). Only when probed by the moderator, some participants tried to connect these issues of data storage back to data collection, elaborating *"that information comes from very many places and may be transmitted. And the more places something comes from and the more it is transmitted, the easier it is to be 'snapped up' by people who should not have access to it"* (P1-I) – i.e. the more complex a dataveillance technology becomes, the more opportunity it may offer for unauthorised access – or, potentially, being tampered with.

In addition, participants outlined that the more data was collected over an extended period of time, the more likely it would be that the collected pool of data contained something that may be used against the respective individual, pointing at data security not being a mere problem of "interior" safety (i.e. storage systems, access rules), but also subject to "exterior" factors such as complexity and time.

Amongst the types of data some of the participants accepted should be gathered (by government agencies) were name, ID, financial information such as income and assets, and – to a limited extent –

health-related data. As unacceptable they indicated in particular sexual orientation, political beliefs, private relationships, private pictures, and location data. Regarding the information gathering by private companies, one participant outlined there should be collected *"only that which is necessary in order to be able to deal with you – and that they do not share it with others"* (P5-I), strongly rejecting any form of commercial "reuse" of – or trading of – personal data.

Another aspect was brought up by some participants of group 3 (45+ years) who, rather than speaking of acceptance as a rational decision, related acceptance to feelings of trust: *"I find that in Norway people place a great amount of trust in the government [...] that the government is right, that we have to follow rules and that we have to adapt [...] questions are never asked"* (P3-III). Providing personal information to government agencies appeared to be accepted, *"because it's a form of communication between the state and the citizens, so they have to have some information"* (P4-III). Although, here, the reference was made to general data provision rather than specifically surveillance data, it shed light on a perspective where surveillance may, in some cases, not be merely seen as an instrument of authoritative power imposed from above, but also as a more power-neutral transfer of information.

5.2.3.3 Perceived effectiveness of smart technologies

Issues of effectiveness were also mentioned by the participants, who predominantly discussed the automatic decision-making process of smart technologies – an issue which appeared to bring up mixed feelings and beliefs. Firstly, they differentiated between decisions taken by humans and those taken by automated technologies. In this regard, a number of participants perceived smart technologies as being *"slightly more scary than the older technologies"* (P4-III). On the other side, particularly participants in group 3 (45+ years) argued that, although *"machines are also developed by people"* (P6-III), decisions would be less prejudiced and carry less *"cultural baggage"* (P3-III). Some of them revealed a certain trust in technology itself, although others in this group expressed their belief that any technological solution would always be limited because of its tendency to result in "black-or-white decisions" which was seen to be against human reality. Additionally, some participants of group 1 (18-24 years) outlined that automation would not necessarily improve data quality, as *"computers are not error-free"* (P4-I). In group 2 (25-44 years), two participants who worked in shops with CCTV surveillance described how "*one gains experience with who actually steals, and we know who they are. As soon as they come in, we follow them"* (P7-II), revealing a certain level of self-awareness (and self-criticism) about such "traditional" surveillance practice: *"In this way, we also collect prejudices"* (P2-II).

However, the potential effectiveness of smart surveillance technologies was also discussed in a quantitative sense. Some participants perceived them as faster and more precise, outlining that more information may produce a better basis for decisions – *"the automation is collecting everything all the time [...] you don't miss anything"* (P3-II) – though it would not necessarily mean that the information quality itself was improved. In contrast, stand-alone "traditional" surveillance techniques based on

human decision were seen to potentially carry the problem that, due to human error, important information may not only be intentionally dismissed but, simply, accidentally missed out.

But as one of the main difficulties with putatively "smart" surveillance technologies, some participants highlighted that any technology would be based in its automated decision-making on human experience and, therefore, would lack the ability to learn genuinely new things – and, also, lack human intuition: *"Someone who is sitting and looking at a camera can pick up on something that smart technology would not have done, regardless of how much it had to work with"* (P6-III). Ultimately, the main strength of smart surveillance technologies was seen as its use as an effective "warning system" which complements rather than substitutes human decisions.

5.3 Security-Privacy Trade-offs

5.3.1 Acceptance of Technological Surveillance

In order to gauge participants' perceptions vis-à-vis a potential 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 of vulnerable groups. The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[4].

Although some participants ascribed some effectiveness to such surveillance measures – *"there is certainly a greater chance of them catching criminals"* (P7-I) – the majority showed a very intense reaction when discussion the scenarios. Particularly participants of group 1 (18-24 years) revealed feelings of deep insecurity: *"It does not give any confidence [security] to the individual at all. It is like a flock of sheep that you have control of, who are labelled, who you have control of at any time"* (P4-I), paired with a certain scepticism that fighting crime would not be the "true" purpose – *"they are using the shooting only as an excuse, in a way, to introduce these measures"* (P6-I). Generally, it was felt that indiscriminate data collection in combination with smart technologies would go *"directly against the principle that everyone is innocent until proven guilty – in this case you are guilty until you are proven otherwise"* (P4-I), violating as such basic human rights.

In contrast, most participants of group 2 (25-44 years) expressed less feelings of insecurity, one specifically outlining that situations of paranoia had somewhat become part of everyday life. But whilst they first agreed that they would not feel personally targeted, the discussion initiated a process of reflection amongst these participants, who started questioning whether or not they themselves would represent a "potential risk" to the general public. However, privacy appeared not to be perceived as something that was either strongly violated or to be traded in.

Finally, one participant of group 3 explained that she would, actually, feel safer in the first scenario, because *"I would have felt that the authorities would have more of an overview"* (P4-III). However, as she elaborated further, *"whether this is achieved is another matter – but I would have felt safer"*. Here, the participant revealed an awareness that perceived safety and actual safety may be different matters – an argument that was taken up further in the subsequent discussion by other participants. Starting out

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

from the point that specific surveillance technologies would provide a false sense of security, they developed the idea that this may result in a generally reduced risk awareness. Ultimately, a false sense of security would be produced through "visible" surveillance measures (such as CCTV cameras) whilst other, less visible forms of surveillance (such as dataveillance) would not work effectively either.

5.3.2 Perception of Different Technologies

Regarding which technologies were accepted or not accepted, it appeared that some participants shared the perception that *"unfortunately we have no choice"* (P3-III), because any of the more subtle surveillance technologies would already be part of everyday life – such as ANPR, CCTV cameras, payment systems, or biometric passports.

Most participants though differentiated in their acceptance between the various surveillance technologies: CCTV cameras and ANPR appeared to be more accepted in all groups – the latter as long as it was incident-triggered (for speed control) or related to a specific purpose (e.g., toll collection). Biometrics would be a question of purpose – and of extent: *"If I am applying for a job and it requires some security, then fingerprints are ok. But having eyes, fingerprints and DNA for everyone – no"* (P5-I). If used for screening entire populations, biometrical surveillance was perceived as the most invasive technology. Geolocation tracking appeared to cause discomfort as well; in particular the geolocation tracking of vulnerable groups such as the elderly or children was seen as problematic, because they may not be capable of giving fully informed consent.

Regarding specific locations where surveillance was accepted, participants predominantly mentioned prisons, airports, borders, and public places where many people accumulate. Surveillance in private companies and workplaces also appeared to be accepted – the latter if required for workplace security, and the former because one would have a choice to go (or not to go) there. In both cases, however, a clear information policy was expected. On the other hand, surveillance in private homes, schools, universities, or nursing homes was strongly rejected. Opinions varied about public spaces that seemed to have a somewhat "semi-private" character – pubs, restaurants and sports facilities.

Ultimately, as some participants explained, it must be possible to move in public space without being constantly under surveillance – *"you can go around if you feel it is offensive"* (P2-II), and *"it is only connected to the one place, it does not follow me around the town"* (P6-II). The specific criticism, here, was aimed at surveillance technologies that are dynamic – which can be seen as one of the core characteristics of smart surveillance.

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 as well as the length and location of data storage.

5.4.1 Effectiveness of laws and regulations

Regarding the effectiveness of privacy laws, the participants' opinions were rather mixed. Particularly participants in group 1 (18-24 years) appeared to feel not sufficiently protected by current legislation, because *"the laws are often broken [by the police]"* (P1-I). Additionally, they felt a lack of effectiveness due to the fact that *"a lot of it is also gathered by foreign operators that do not need to comply with Norwegian laws"* (P5-I). Similarly, participants in group 2 (25-44 years) who did express a rather *"decent trust in that the Norwegian state will look after my information in the way it should be done"* (P3-II) outlined that this trust was focussed on Norway and explicitly did not comprise *"other countries that are out there which are a bit less democratic"* (P3-II).

Additionally, some participants declared their impression that private Norwegian companies *"are much stricter than I would have expected from them"* (P3-II), in sharing personal information with public authorities. Generally, there appeared to be a strong desire to have a regulation that requires a court order to request or release personal information, and the perception that there were unclear regulations regarding the "reuse" of information, i.e. usage for a purpose that differs from the one the information was originally gathered for.

In contrast, some participants in group 3 (45+ years) showed a rather strong trust in the effectiveness of Norwegian privacy laws, though grounding this on a feeling rather than direct experience: *"I think that the Data Protection Authority works. I like the Data Protection Authority – I don't know why"* (P3-III). At the same time, they outlined that *"with more technology things must be stricter in order to protect people's privacy. But we have some lawyers, as well as authorities, who are largely trusted and will take care of it. I hope"* (P4-III). Such projection of trust in future developments allows, perhaps, for the assumption that these participants, despite their active and critical attitude, feel quite comfortable with the current situation.

5.4.2 Location and length of data storage

Regarding storage location, a number of participants strongly expressed their belief that citizens' personal data should not be stored by one centralised (public) entity: *"If one entity has all the information that is possible to collect a society of profiles is created"* (P3-III). They also showed a rather strong trust in the Norwegian data protection authority, understood as protecting not only data but also citizens' interests. The general perception was focused on three cornerstones of data protection: *"The*

data protection authority as a controlling body, [...] not having all information collected [stored] in one place, and [...] there must be a time limit [for data storage]" (P3-III).

Regarding the length of storage for surveillance data, the storage period for personal data was perceived as a generally important factor, because *"it is more problematic that something can be used against you for the rest of your life than for the next year"* (P6-II) – and, consequently *"the longer it is stored, the more unsafe I would feel"* (P3-I). There was also general agreement amongst the participants that unlimited data storage was not acceptable and there should be a set time limit for data storage. Here, however, the participants' suggestions ranged between one month and one year.

But storage length should also be defined and limited by usage – *"once they have used it for the purpose it has to be used for, it should be deleted"* (P5-I) – particularly biometric information that was collected in specific situations (such as border control), was expected to be either deleted immediately or kept only for a very short time. Other participants distinguished between different surveillance measures: For data recorded by CCTV cameras, a storage period between three weeks and three months was suggested. However, they were also aware that *"the shorter the period the less useful it is"* (P6-III).

6. Conclusion: Between Care and Concern – *"Are we sure we know the rules?"*

Although intentional data misuse appeared not to be at the top of most participants' minds, their main concerns in the context of personal data collection (from surveillance or otherwise) on a massive scale and in combination with long-term storage were twofold: They did perceive generally increased data security issues, but what appeared to worry them more was the gradual build-up of a complex data-based "digital collective memory" which may not be as merciful and forgiving as human memory.

As protection against the first concern, participants highlighted the need for a strong and independent data protection authority. The discomfort related to the second issue, despite a rather strong trust in the Norwegian government, appeared to run deeper and, partially, influenced by perceptions of local history:

> *"I can imagine that this [data collection] isn't only about plane tickets, because it isn't that long ago since this country was occupied, and it can be used politically. There were mass registers everywhere, right?*[5] *So I think that's also a bit of a far-fetched perspective, hopefully, but..."* (P1-III).
> *"What you brought up is: What is done with such a register in a crisis situation? That's when it becomes dangerous. [...] So the question is: Are we really sure we know the rules?"* (P6-III).

The aforementioned trust in the Norwegian state as a welfare-oriented social institution seemed also to be shaken by some participants' perception that control – rather than care – is increasingly becoming a central interest of public authorities: *"We have immense trust in the Norwegian government – we grow up thinking it is there for us. And then things start appearing that make you a little scared, too: that people with dementia will be given a GPS. Because that means that we do not have enough people in place"* (P6-III). This could be interpreted that trust in the government is grounded in a government's personal care for its citizens, i.e. people being there for people – and that such care can be substituted by surveillance technologies only to a limited extent.

[5] Reference to the occupation of Norway by Nazi Germany during the 2nd World War.

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

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

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

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

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

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

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

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

- ☐ Yes
- ☐ No

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

- ☐ **Yes**
- ☐ **No**

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

- ☐ Yes
- ☐ No

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

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

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

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

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

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

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

Scenario 1: Supermarket

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

Scenario 2: Travelling

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

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

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

Scenario 4: Mobile devices

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

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

Aims:

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

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

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?***

3. Explore the participants' understanding of where their information is ending up	***b. Where do you think your personal information will end up?***
	4. <u>Why</u> the information is being recorded, collected and stored:
	a. Why do you think your personal information is being recorded and collected?
	b. In what ways do you think your personal information will be used?
	Running Total: 35min
Presentation of cards depicting different technologies and applications [10mins] *To expose participants to a selection of relevant SMART technologies & applications in order to enable a better understanding and hence to facilitate the discussion.*	***Item 3*** *Present the following three cards (each depicting a group of different technologies and applications) to the group. The cards will include the following depictions:* ***Card 1 – Person or event recognition & tracking technologies**: Automated moving of closed circuit television (CCTV) cameras; Automatic number plate reader (ANPR) or automatic vehicle number identification (AVNI); and tracking devices such as mobile phone tracking and RFID* ***Card 2 - Biometrics**: Biometric technologies including fingerprint and iris scanning; and automatic facial recognition (AFR)* ***Card 3 - Object and product detection devices**: Knife arches (portal) and X-ray devices* ***Running total: 40min***
Presentation of MIMSI scenario to participants **[30mins]** - *To explore participants' understanding of the implications of MIMSI* - *To explore participants' feelings, beliefs and attitudes vis-à-vis the sharing of personal*	***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*

information	*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'...*
Aims *1. Participants' first*	***Mr. Brown**: I am...goodbye...* *After presenting the previous scenario to the group, probe in-depth to*

reactions including: *Possibility / impossibility of scenario* *Acceptability / unacceptability of scenario* *2. Participants' beliefs and attitudes on how technology affects or might affect their privacy* *3. Participants' beliefs and attitudes in terms of the type of information such as: Medical & financial data; photos and location.* *4. Participants' beliefs and attitudes on the collection, usage and sharing of personal information with third parties.* *5. Participants' beliefs and attitudes on the benefits and drawbacks of being monitored*	*explore the following:* ***1a. How would you feel if this happened to you?*** *(Also probe to establish the degree of control / helplessness felt by the participants in such a hypothetical scenario)* ***1b. How would you react if this happened to you? What would you do?*** ***1c. Is such a scenario possible / impossible?*** ***1d. Is such a scenario acceptable / unacceptable?*** ***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*	***Item 5*** **During the next exercise, we will be discussing the following hypothetical scenario. Imagine the following scenario:**

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

- *Here, the discussion should not focus on whether these technologies will increase security - this should be taken as a given. The discussion should mainly centre on whether these technologies effect privacy and hence revolve around the security - privacy trade-off*

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

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 safe in the scenario provided?

1b. What makes you feel vulnerable 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

2. From the smart technologies depicted in the scenario, i.e.

specific technologies	***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)***
3. Locations of deployment such as: *Airports* *Malls* *Streets*	***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?*** ***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]	***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***

▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***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 (NORWEGIAN)

Presentasjon	Orientering
Velkommen til deltakerne - *Hils på deltakerne* - *Utdeling av navnelapper* - *Underskriving av samtykkeskjemaer*	*Ønsk deltakerne velkommen med det samme de kommer inn. Vis dem hvor de skal sitte og gi dem en navnelapp.* *Del ut samtykkeskjemaet til deltakerne og be dem lese og skrive under skjemaet før fokusgruppen begynner. Dette er viktig, slik at deltakerne forstår hva de samtykker til.*
Innføring [rundt 10 minutter] - *Takk* - *Presentasjon av tilretteleggingsteamet Formål* - *Fortrolighet* - *Varighet* - *Grunnregler for gruppen* - *Kort presentasjon av deltakerne*	**Velkommen til denne fokusgruppen og takk for at dere ville delta i denne økten. Vi er glade for at dere tok dere tid til å delta i dette prosjektet, og setter stor pris på at dere involverer dere på denne måten.** **Jeg heter _____ og skal legge til rette for gruppesamtalen. Jeg får hjelp av _____ som er moderator sammen med meg og vil ta notater og ta opp samtalen på bånd.** *Presenter eventuelle andre kolleger som er til stede* **Denne økten vil ta mellom halvannen og to timer, og ettersom vi tar opp samtalen på bånd, er det fint om dere snakker tydelig; synspunktene og tankene dere har, er svært viktige for denne forskningen, så vi vil helst ikke gå glipp av noe dere sier.** **Som før nevnt da dere først ble bedt om å delta i denne samtalen, handler denne fokusgruppen om teknologi og personvern, og blir utført som en del av SMART-prosjektet, som er delvis finansiert av EU-kommisjonen. For de av dere som ønsker å vite mer om SMART-prosjektet, er det bare å gi oss beskjed, så skal vi sørge for å gi dere mer informasjon når fokusgruppen er slutt.** *På dette steget er det viktig å ikke røpe ytterligere detaljer om innholdet i fokusgruppen, slik at vi unngår å påvirke samtalen som følger.* **Som dere ble informert om da dere leste og skrev under samtykkeskjemaet, skal alt som tas opp på bånd i løpet av denne økten, holdes fortrolig, og dere vil være anonyme. Det vil si at kommentarene deres bare blir delt med de som er involvert i denne studien og brukt i vitenskapelige publikasjoner fra denne studien, og de blir anonymisert før de inngår i noen rapportering. Opplysninger som inngår i rapporten vil derfor ikke identifisere dere som deltakere på noen måte. For å få til dette får hver av dere tildelt et nummer, og det er dette nummeret som blir brukt i rapporten.**

	Jeg ønsker også å forsikre meg om at alle i gruppen synes det er greit å dele synspunktene sine. For at dette skal være mulig, vil jeg be hver og én som er til stede om å følge disse grunnreglene: ▪ **Vi vil gjerne høre fra alle i gruppen – vi er interessert i synspunkter fra alle** ▪ **Det er ingen riktige eller gale svar, så la oss være enige om å respektere hverandres oppfatninger** ▪ **Sørg for at alle mobiltelefoner er stille, slik at samtalen ikke blir avbrutt.** ▪ **Det er viktig at kommentarer gjøres én av gangen, ettersom synspunktene til alle deltakerne er viktige. La oss derfor være enige om å ikke snakke i munnen på hverandre, ellers blir det vanskelig å få med oss alt som blir sagt i løpet av økten.** ▪ **La oss være enige om at vi som gruppe respekterer hverandres fortrolighet, slik at alle synes det er greit å snakke fritt.** **Dersom det er noen andre som vil foreslå andre grunnregler, er det bare å legge fram forslagene deres for gruppen.** **Er det noen som har spørsmål før vi starter?** **OK, la meg da begynne med å be dere presentere dere kort for gruppen uten å røpe private opplysninger. La oss ta en runde der dere forteller hva dere heter og kanskje litt om dere selv. Jeg starter med meg selv …** ***(ta en kort presentasjonsrunde)*** *Total tid: 10 min*
Mål	**Samtaleemner og øvelser**
Øvelse med ordassosiasjon **[rundt 5 minutter]** *- En ordassosiasjonslek er med på å bryte isen* *- Klarlegg de første assosiasjonene med hovedtemaene* *- Start gruppesamtalen*	***Punkt 1*** **Først skal vi leke en liten lek: Jeg skal lese opp et ord, og så vil jeg at dere sier de første tingene dere tenker på når dere hører dette ordet. La oss ta et eksempel først: Hva er det første dere tenker på hvis jeg sier ordet «*mat*»? Prøv helst å tenke på enkeltord eller korte setninger, og unngå lange beskrivelser.** *Les opp (ett av gangen):* *Teknologi, personvern, nasjonal sikkerhet, personopplysninger, personlig sikkerhet* *Total tid: 15 min*

Samtale om dagligdagse erfaringer knyttet til overvåking

[20 min]

-Å utforske deltakernes erfaring med overvåking og hva de tenker om det

-Å utforske deltakernes kjennskap til og kunnskap om ulik overvåkingsteknologi

Punkt 2

La oss snakke om noe annet. Jeg vil at dere skal tenke på situasjoner der dere føler at dere eller det dere gjør blir observert, samt eventuelle situasjoner der dere er klar over at det blir innsamlet opplysninger om dere. La oss begynne med å tenke på aktiviteter dere gjør til vanlig. La oss ta følgende situasjoner som eksempler på dette.

Scenario 1: Dagligvarebutikk

Som et første eksempel kan vi se på en handletur i den vanlige dagligvarebutikken din. Kan dere dele tankene dere gjør dere om dette?

Scenario 2: Reise

La oss gå videre til en annen situasjon, denne gangen relatert til reiser. Hva med når dere reiser med fly?

Scenario 3: Offentlige steder (f.eks. museer, stadioner)

Forestill dere nå at dere besøker et offentlig sted, f.eks. et museum, eller er på et arrangement som f.eks. en fotballkamp eller en konsert. Hva slags aktiviteter tror dere blir registrert?

Scenario 4: Mobile enheter

La oss snakke om ett siste eksempel. Tenk på de gangene dere bruker mobiltelefon. Hva tror dere blir registrert i dette tilfellet?

Mål:

1. Å utforske deltakernes kjennskap til og kunnskap om teknologien

2. Å utforske deltakernes erfaring med å bli overvåket i sine mange roller

3. Å utforske deltakernes forståelse av hvor informasjonen ender opp

4. Å utforske

Prøv i hvert enkelt tilfelle å utforske følgende i detalj, der det er mulig:

1. ***Hvordan opplysninger samles inn:***
    a. ***Hva slags teknologi tror dere blir brukt til å samle inn personopplysninger?***
2. ***Hva slags opplysninger samles inn:***
    a. ***Hva slags personopplysninger tror dere samles inn?***
3. ***Hvem samler inn opplysningene:***
    a. ***Hvem tror dere er ansvarlig for å samle inn og registrere personopplysninger om dere?***
    b. ***Hvor tror dere personopplysningene deres ender opp?***
4. ***Hvorfor opplysningene registreres, samles inn og lagres:***

deltakernes synspunkter på hvorfor det de gjør blir observert, overvåket og nnsamlet

a. ***Hvorfor tror dere personopplysningene deres blir registrert og innsamlet?***

b. ***Hva slags måter tror dere personopplysningene deres blir brukt på?***

Total tid: 35 min

Presentasjon av kort som viser ulik teknologi og ulike bruksområder [10 min]

Å vise deltakerne et utvalg relevant SMART-teknologi og bruksområder for å gi en bedre forståelse og dermed lette samtalen.

Punkt 3

Vis fram følgende tre kort (hvert av dem viser en gruppe med ulik teknologi og ulike bruksområder) til gruppen. Kortene viser følgende framstillinger:

***Kort 1 – Teknologi for gjenkjenning og sporing av personer og hendelser**: Automatisert flytting av overvåkingskameraer, automatisk nummerskiltleser eller automatisk registreringsnummeridentifisering, samt sporingsutstyr som mobiltelefonsporing og RFID*

***Kort 2 – Biometri**: Biometriteknologi omfatter scanning av fingeravtrykk og iris, samt automatisk ansiktsgjenkjenning*

***Kort 3 – Objekt- og produktdetektorer**: Metalldetektorer (portaler) og røntgenapparater*

Total tid: 40 min

Presentasjon av MIMSI-scenariet for deltakerne

[30 min]

- *Å utforske deltakernes forståelse av hva MIMSI innebærer*

- *Å utforske deltakernes følelser, oppfatninger og holdninger til å gi fra seg personopplysninger*

Punkt 4

Presenter følgende hypotetiske scenario for gruppen. En innspilling av telefonsamtalen kan forberedes og presenteres for gruppen.

Telefonsamtale med kundebehandleren ved hovedkontoret i NAV

***Kundebehandler**: Hei, dette er Kari. Hvordan går det med deg, Ola? Vi har ventet på at du skulle ringe etter at arbeidskontrakten din tok slutt for en måned siden.*
***Ola**: Øh… ja, det er faktisk derfor jeg ringer …*
***Kundebehandler**: Ja, jeg er ikke overrasket over at du ringer først nå … hvordan var ferien på Kypros? Jeg håper kona og barna likte hotellet dere bodde på …*
***Ola**: Ja, det var en fin ferie … og hvordan vet du det?*
***Kundebehandler**: Å, det ligger i systemet, det, Ola … så klart. Uansett – det ville vært fint å komme i gang med å søke arbeid …hva med utgiftene for ferien og avbetalingen på bilen som kommer snart … for ikke å snakke om innbetalingen på kredittkortet den 22. denne måneden …*
***Ola**: Ligger det også i systemet deres?*
***Kundebehandler**: Ja, selvfølgelig, Ola. Forresten, det var en fin bok du kjøpte på Internett … jeg har lest den selv og fant mange gode tips der …*
***Ola**: Hm… okei … når det gjelder denne nye jobbsøkertjenesten, trenger jeg å sende inn et oppdatert bilde av meg selv?*
***Kundebehandler**: Neida, Ola, det er jo alt på plass! Vi har mange nye bilder i systemet vårt. Fin farge du fikk i ferien, forresten! Været var nok bra! Og før jeg glemmer det: Når det gjelder bildet, vil du ha et med eller uten briller?*
***Ola**: Å… tja … uten går bra … så registreringen min – kan vi sette opp en avtale i neste uke?*
***Kundebehandler**: Jeg skal se i systemet … hva med onsdag klokka 12? Nei, vent litt! Jeg så akkurat at du har time hos legen akkurat da. Du vil sikkert ikke hoppe over den, så viktig som det er å passe på kolesterolnivået sitt! Hva med torsdag morgen klokka 9?*
***Ola**: Torsdag morgen er bra … må jeg ta med meg noe dokumentasjon?*
***Kundebehandler**: Neida, Ola, vi har allerede alle opplysninger vi trenger i systemet vårt.*
***Ola**: Sikkert …*
***Kundebehandler**: Takk for at du ringte, Ola, så ser vi deg neste uke. Og kos deg med cappuccinoen på Café Olé …*
***Ola**: Det skal jeg gjøre … ha det …*
…

Mål

Presenter det foregående scenariet for gruppen og sonder grundig etter det følgende:

1. Deltakernes første reaksjoner inkludert: Hvor mulig/umulig

1a. Hvordan ville dere følt det om dette hadde hendt med dere?
(Prøv også å bringe på det rene graden av kontroll/hjelpeløshet

scenariet er
Hvor akseptabelt/ uakseptabelt scenariet er

2. Deltakernes oppfatninger og holdninger til hvordan teknologi påvirker eller kan påvirke personvernet deres

3. Deltakernes oppfatninger og holdninger til ulike typer informasjon som: Pasientopplysninger; Økonomiske opplysninger; bilder og steder.

4. Deltakernes oppfatninger og holdninger til innsamling, bruk og å gi fra seg personopplysninger til tredjeparter.

5. Deltakernes oppfatninger og holdninger til fordelene og ulempene ved å bli overvåket

som deltakerne føler i et slikt hypotetisk scenario)

1b. Hvordan ville dere reagert om dette hadde hendt med dere? Hva ville dere gjort?
1c. Er et slikt scenario mulig/umulig?
1d. Er et slikt scenario akseptabelt/uakseptabelt?

2a. I hvilken grad tror dere «stand alone» (enkeltstående teknologi) påvirker personvernet deres?
2b. I hvilken gard tror dere «smart teknologi», dvs. teknologi som prosesserer data på en automatisk (eller halvautomatisk) måte, påvirker personvernet deres?

3a. Hva slags personopplysninger synes dere det er greit at blir innsamlet, brukt og/eller delt med andre?
3b. Hva slags personopplysninger ville dere motsatt dere at blir innsamlet, brukt og/eller delt med andre?

4a. Hva synes dere om at personopplysninger om dere blir innsamlet, brukt og delt av staten?
4b. Hva synes dere om at personopplysninger om dere blir innsamlet, brukt og delt av private (f.eks. kommersielle aktører)?

5a. Synes dere det er fordeler knyttet til at det dere gjør blir overvåket?
5b. Synes dere det er ulemper knyttet til at det dere gjør blir overvåket?

Total tid: 1 time 15 min

Reaksjoner på scenariene

[rundt 20 minutter]

- *Å stimulere til debatt for å utforske deltakernes oppfatninger av «kompromiss mellom sikkerhet og personvern».*

- *Samtalen bør ikke dreie seg om hvorvidt denne teknologien vil gi økt sikkerhet – det må tas for gitt. Samtalen bør hovedsakelig dreie seg om hvorvidt denne teknologien påvirker personvernet og derfor ta for seg kompromisset mellom sikkerhet og personvern.*

Mål:

1. Sikkerhetsklima og trusselnivå

Punkt 5

I neste øvelse skal vi snakke om følgende hypotetiske scenario. Forestill dere følgende scenario:

På grunn av en betydelig økning i *voldelig kriminalitet* i hovedstaden, blant annet *en bølge med kidnappinger og mord som synes tilfeldige og uten sammenheng*, har staten bestemt seg for å bruke overvåkningskameraer på alle offentlige steder, både de som er eid av det offentlige (som t-banestasjoner, parker osv.) og de som er eid av private (som butikker, shoppingsenter og drosjer), som gjør det mulig med automatisk ansiktsgjenkjenning. I tillegg blir nummerskiltet på alle biler som kjører gjennom hovedfartsårene, registrert. Det er også planer om å installere sensorer på alle offentlige steder, som kan oppdage høy lyd, f.eks. når noen skriker. Alle borgere blir avkrevd DNA og fingeravtrykk, og scanning av iris. Staten har også bestemt at alle borgere som blir identifisert som en mulig risiko for andre, skal ha elektronisk merking for å overvåke og spore bevegelsene deres. For deres egen sikkerhet blir også gamle og barn opptil 12 år elektronisk merket. Alle data fra den ulike teknologien blir lagret i sammenknyttede databaser som administreres av politiet, som blir automatisk varslet dersom det er grunn til alarm og risiko for noen av borgerne.

Be deltakerne forestille seg scenariet ovenfor, men med følgende varianter:

Variant 1: Selv om det har vært en betydelig økning i voldelig kriminalitet i de fleste byene omkring, har det ikke vært noen økning i kriminaliteten i byen du bor i. Staten har likevel bestemt seg for å innføre overvåkingen som et forebyggende tiltak.

Variant 2: Hele landet har generelt svært lav kriminalitet, men staten bestemmer seg likevel for å innføre overvåkingen som et forebyggende tiltak etter at en naboby opplevde en isolert hendelse der flere personer ble skutt og alvorlig skadet av en mann som begynte å skyte på et shoppingsenter.

Under samtalen om scenariet/variantene ovenfor må du sondere grundig etter følgende faktorer og hva de kan ha å si for «kompromisset mellom sikkerhet og personvern»:

1a. Hva får dere til å føle dere trygge i det gitte scenariet?

1b. Hva får dere til å føle dere sårbare i det gitte scenariet?

2. Bruk av spesifikk teknologi

3. Bruksteder som f.eks.:
Flyplasser
Shoppingsenter
Gater

4. Eksistensen av lover og andre forholdsregler (i forbindelse med innsamling, lagring og bruk av data)

5. Hvor lenge overvåkingsdata kan lagres

1c. Ville dere vært villige til å gi avkall på personvernet deres dersom trusselnivået var annerledes, som i variant 1 og 2 av scenariet?

2. Av den smarte teknologien beskrevet i scenariet, dvs.
overvåkingskameraer med automatisk ansiktsgjenkjenning,
automatisk gjenkjenning av nummerskilt,
sensorer (som kan oppdage høy lyd),
biometrisk teknologi (inkludert fingeravtrykk) og
elektronisk merking (med bruk av RFID)

2a. Hvilken teknologi synes dere er akseptabel? Hvorfor?
2b. Hvilken teknologi synes dere er invasiv og en trussel mot personvernet deres? Hvorfor?
2c. Hva synes dere om denne automatiserte (halvautomatiserte) teknologien der den endelige avgjørelsen blir tatt av systemet og ikke av en person som styrer den?
3a. Hvilke steder synes dere det er akseptabelt å bli overvåket på? Hvorfor?
3b. Hvilke steder synes dere det er uakseptabelt å bli overvåket på?
4a. Hva synes dere om personvernlovgivningen? Får den dere til å føle dere beskyttet?

4b. Er det noen forholdsregler eller vilkår som dere ville synes var betryggende?

5a. Hva synes dere om varigheten av lagringstiden for overvåkingsdata? Spiller det noen rolle?
For å hjelpe til med sonderingen kan du gi deltakerne følgende eksempler:
- ***Opptak fra overvåkingskameraer***
- ***Lokalisering og bevegelser av biler***
- ***Lagring av DNA, fingeravtrykk og irisscanning***
- ***Lokalisering av personer som utgjør en risiko for andre***
- ***Lokalisering og bevegelser av gamle og barn***

5b. Dersom lengden av lagringen spiller noen rolle, hva synes dere er en akseptabel tidsramme?

Total tid: 1 time 35 min

Mål	Oppsummeringsøkt
Kort sammendrag av samtalene [5 min] - *Å bekrefte hovedpunktene som er framkommet* - *Å gi en ekstra mulighet til å utbrodere det som ble sagt*	*Punkt 6* *På slutten av fokusgruppen er det nyttig å gi et sammendrag av punktene som kom fram. Her bør du ta sikte på å gi en kort oppsummering av temaene og sakene som ble tatt opp i løpet av samtalene. Etterpå kan du spørre deltakerne om dette:* - «Hvor godt fanger dette opp det som ble sagt her i dag?» - «Er det noe vi har oversett?» - «Har vi dekket alt?» *Denne korte økten gir deltakerne en ekstra mulighet til å uttrykke det de mener, og kan også brukes til å utbrodere ting som ble tatt opp, men som ikke ble fulgt opp ved den anledningen.* ***Total tid: 1 time 40 min***

Mål	Avslutning
Avslutning av fokusgruppen [5 min] ▪ ***Å takke deltakerne*** ▪ ***Å dele ut godtgjørelse*** ▪ ***Å gi informasjon om SMART***	***Punkt 7*** **Med denne siste øvelsen er vi i havn med samtalene. Vi vil benytte denne anledningen til å takke dere enda en gang for at dere ble med oss og delte deres synspunkter, erfaringer og tanker.** ***Del nå ut godtgjørelse til deltakerne og informer dem om de neste stegene.*** ***Gi mer informasjon om SMART til deltakerne som ba om dette.*** ***Total tid: 1 time 45 min***

APPENDIX D – DEBRIEFING FORM

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

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

APPENDIX E – CONSENT FORM

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

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

1.1. Commercial space

1.1.1. Awareness of different surveillance methods/technologies

1.1.1.1. CCTV

1.1.1.2. Financial monitoring

1.1.1.3. Loyalty cards

1.1.2. Perceived purposes

1.1.2.1. Marketing

1.1.2.2. Prevention and prosecution of theft

1.2. Boundary space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. Monitoring of personal data

1.2.1.1.1. Personal and travel-related data

1.2.1.1.2. Financial monitoring

1.2.1.1.3. Biometric data in passports

1.2.1.1.4. Behavioural data (shopping habits)

1.2.2. Perceived purposes

1.2.2.1. National security

1.2.2.2. Marketing purposes

1.2.2.3. Business strategy

1.2.2.4. Border control

1.2.2.5. Exploitation of data

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV

1.3.1.2. Security guards

1.3.1.3. Monitoring of data through ticket purchase

1.3.2. Perceived purposes

1.3.2.1. Protection of goods

1.3.2.2. Crowd control

1.3.2.3. Marketing

1.3.2.4. Prevention of fraud

1.3.2.5. Security

1.4. Mobile devices and virtual spaces

1.4.1. Awareness of different surveillance methods/technologies

1.4.1.1. Geolocation tracking

1.4.1.2. Data monitoring on social networks

1.4.2. Perceived purposes

1.4.2.1. Collection of telecommunication data

1.4.2.2. Collection of GPS data
1.4.2.3. Security

2. Perceptions and attitudes towards smart surveillance and integrated dataveillance

2.1. Feelings
2.1.1. Extreme discomfort
2.1.1.1. Lack of control
2.1.1.2. Fear
2.1.1.3. Violation of boundaries
2.2. Behavioural intentions
2.2.1. Active reactions
2.2.1.1.1. Take independent action
2.2.1.2. Passive reactions
2.2.1.2.1. Helplessness
2.2.1.2.2. Paranoia
2.3. Beliefs
2.3.1. Likelihood of smart surveillance and massively integrated dataveillance
2.3.1.1. Technical aspect
2.3.1.2. Legal aspect
2.3.2. Acceptance of massively integrated dataveillance
2.3.2.1. Purpose of surveillance
2.3.2.2. Data security
2.3.2.3. Type of data
2.3.2.4. Data sharing
2.3.2.5. Trust into the government
2.3.3. Perceived effectiveness of smart technologies and dataveillance
2.3.3.1. Decision-making capabilities of automated systems
2.3.3.1.1. Neutrality aspect of machine programming
2.3.3.1.2. Wrong conclusions and deficiency of machines
2.3.3.1.3. Human aspect

3. Security-privacy trade-offs

3.1. Acceptance of technological surveillance
3.1.1. Feelings
3.1.1.1. Deep insecurity
3.1.1.2. Scepticism
3.1.1.3. Paranoia
3.1.1.4. Safety
3.1.2. General beliefs
3.1.2.1. Violation of rights
3.1.3. Effectiveness of surveillance

- 3.1.3.1. Perceived safety and actual safety
- 3.1.3.2. Risk awareness

3.2. Perceptions of different technologies

- 3.2.1. CCTV
  - 3.2.1.1. Acceptance
- 3.2.2. ANPR
  - 3.2.2.1. Acceptance for specific purposes
- 3.2.3. Biometric data
  - 3.2.3.1. Question of purpose
  - 3.2.3.2. Extent
  - 3.2.3.3. Invasiveness
- 3.2.4. GPS tracking
  - 3.2.4.1. Useful for the monitoring of children
  - 3.2.4.2. Infringement of privacy and right of free movement
- 3.2.5. Locations of deployment
  - 3.2.5.1. Places with many people
  - 3.2.5.2. Private spheres
  - 3.2.5.3. Public space

4. Surveillance laws and regulations

4.1. Feelings and beliefs

- 4.1.1. Effectiveness of laws and regulation
  - 4.1.1.1. Protection by current legislation
  - 4.1.1.2. Lack of effectiveness
  - 4.1.1.3. Need of stricter regulations
  - 4.1.1.4. Trust into laws
- 4.1.2. Location and length of data storage
  - 4.1.2.1. Centralization of data
  - 4.1.2.2. Trust into the Norwegian data protection authority
  - 4.1.2.3. Limited data storage time and usage
  - 4.1.2.4. Different storage for different types of data